DERECHO A LA PRIVACIDAD Y SEGURIDAD EN EL ESPACIO PÚBLICO EUROPEO

Giuseppe Rizzo

Tesis depositada en cumplimiento parcial de los requisitos para el grado de Doctor en

Derecho

Universidad Carlos III de Madrid

Director:

Dr. José Vida Fernández
Dr. Pablo Zapatero Miguel

Tutor:

Dr. José Vida Fernández
Dr. Pablo Zapatero Miguel

Fecha de la defensa de tesis

A mi mismo

AGRADECIMIENTOS

Esta tesis es fruto de años de inestimables esfuerzos, sacrificios, perseverancia y muchísimas renuncias como del apoyo de muchas personas e instituciones que hicieron posible su realización. Por la pasión que tengo por la investigación y la educación universitaria, este doctorado ha sido conseguido sin ayudas económicas, por mi cuenta.

A mi esposa Gabriella, por su amor, apoyo en los momentos más difíciles y la comprensión mostrada a pesar del tiempo robado, sin el cual esta tesis no habría visto la luz.

A nuestra pequeña hija Silvia, que ha nacido durante el último año de esta tesis, lo que me hizo sentir la maravilla de ser padre y me dió las fuerzas necesarias para llegar a puerto.

A mis padres, ellos han sido mis pilares, me lo han dado todo y sin ellos este trabajo no habría llegado nunca.

A mis directores José y Pablo, por sus paciencia, disposición y eruditos consejos. Su profesionalidad unida a sus cualidades personales les hacen merecedores de mi más profundo reconocimiento.

A mis queridos amigos, especialmente a Rubén y Adriana, Sergio y Clara, Raúl y Helena, Elena, Victoria, Alfonso, Celia, así como a Padre José, Padre Antonio y Padre Jesús, a Juan, Fernando y José, por sus cariño, amistad y apoyo en este camino académico en Madrid.

A mi *alma mater*, la Universidad Carlos III de Madrid, en particular a la Escuela de Doctorado y a su personal, por el soporte y colaboración brindado desde el inicio de este proyecto.

A los profesores del Programa de Doctorado en Derecho, en particular Tomás de la Quadra-Salcedo Fernández del Castillo, Óscar Celador Angón, María Nieves de la Serna Bilbao Y Antonio Fortes Martín, y a mis compañeros, por los consejos y buena disposición en el proceso de mi tesis.

A Judith Alexandra González Pedraz y Rafael García Gozalo, Vocal Asesor Jefe del Área Internacional de la AEPD, para orientarme en el comienzo de esta tesis.

A los miembros del Tribunal, que con sus observaciones harán que este trabajo sea aún más completo, lo que significa un gran incentivo y motivación, contribuyendo de una forma relevante en mi formación profesional, académica y personal.

A España y su gente, por haberme hecho sentir en casa, por las oportunidades académicas y por haberme permitido realizar proyectos. Por ello, hoy estoy orgulloso de ser italiano y por haber adoptado, voluntariamente y sentimentalmente, España como mi segunda patria.

Del discurso de *Lord* Chatham ante el Parlamento británico el 27 de marzo de 1763, en defensa de la privacidad de todo ciudadano: «*The poorest man may, in his cottage, bid defiance to all the forces of the crown. It may be frail, its roof may shake, the wind may blow through it, the storm may enter, the rain may enter; but the king of England cannot enter! All his force dare not cross the threshold of the ruined tenement*»*. William Pitt, 1st Earl of Chatham, speech in the British Parliament (March 1763).

*«*El hombre más pobre puede, en su casa, desafiar a todas las fuerzas de la Corona. Esa casa puede ser endeble, su tejado puede derrumbarse, el viento puede soplar en su interior, la tormenta puede entrar, la lluvia puede entrar. Pero el Rey de Inglaterra no puede entrar, sus ejércitos no se atreverán a cruzar el umbral de la arruinada morada*».

«*Nec ad imperii securitatem refert, quo animo homines inducantur ad res recte administrandum, modo res recte administrentur; animi enim libertas, seu fortitudo privata virtus est; at imperii virtus securitas*»*. Spinoza, Tratado Politico, Capítulo I, § 6.

*«*Pues para la seguridad del Estado no importa qué impulsa a los hombres a administrar bien las cosas, con tal que sean bien administradas. En efecto, la libertad de espíritu o fortaleza es una virtud privada, mientras que la virtud del Estado es la seguridad*». (traducción de Atilano Domínguez, Spinoza: Tratado político, Madrid, Alianza Editorial, 1986, pág. 82).

CAPÍTULO I

ALCANCE Y LIMITACIONES DE LA PROTECCIÓN JURÍDICA A LA PRIVACIDAD EN LA ESCENA INTERNACIONAL

CAPÍTULO II

EQUILIBRAR LA PRIVACIDAD Y LA SEGURIDAD NACIONAL EN LOS SISTEMAS CONSTITUCIONALES DE LA UNIÓN EUROPEA HASTA LA NUEVA REFORMA DE LA PROTECCIÓN DE DATOS

CAPÍTULO III

LOS SISTEMAS DE GESTIÓN DE LA INFORMACIÓN DEL ESPACIO EUROPEO DE LIBERTAD, SEGURIDAD Y JUSTICIA Y LA PROTECCIÓN DE DATOS

CAPÍTULO IV

LA TENSIÓN ENTRE PRIVACIDAD Y SEGURIDAD EN LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

CAPÍTULO V

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LA DIRECTIVA DE PROTECCIÓN DE DATOS EN LOS SECTORES POLICIAL Y JUDICIAL. LOS NUEVOS LÍMITES DE ESTADO A LA LIBERTAD EN EUROPA

ABREVIATURAS Y ACRONIMOS

ACNUDH	Alta Comisionada de las Naciones Unidas para los Derechos Humanos
AEPD	Agencia Española de Protección de Datos
APEC	Foro de Cooperación Económica Asia Pacífico
ARCO	Acceso, Rectificación, Cancelación y Oposición
BCE	Banco Central Europeo
BCR	Binding Corporate Rule
BOE	Boletín Oficial del Estado
CAAS	Convenio de Aplicación del Acuerdo Schengen
CAHDATA	Comité ad hoc data
CBPR	Cross Border Privacy Rules
CdE	Consejo de Europa
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales
CEE	Comunidad Económica Europea
CEPOL	Agencia de la Unión Europea para la Formación Policial
CETS	Council of Europe Treaty Series
CIA	Central Intelligence Agency
COM	Comunicación de la Comisión Europea
Convenio n. 108	Convenio para la protección de las persones con respecto al tratamiento automatizado de datos de carácter personal
COREPER	Comité de Representantes Permanente
C-SIS	Central Schengen Information System
DHS	Department of Homeland Security
DPO	Data Protection Officer
DUDH	Declaración Universal de los Derechos Humanos
EC3	Centro Europeo de Ciberdelincuencia de Europol
ECRIS	Sistema Europeo de Información de Antecedentes Penales
ECTC	Centro Europeo Contra el Terrorismo
EDPS	European Data Protection Supervisor
EE.UU.	Estados Unidos
EEE	Espacio Económico Europeo

EIPD	Evaluación de Impacto en la Protección de Datos personales
ELSJ	Espacio de Libertad, Seguridad y Justicia
ENISA	Agencia de Seguridad de las Redes y de la Información de la Unión
Europea SOCTA	Serious and Organised Crime Threat Assessment
eu-LISA	EU Agency for Large-scale IT Systems
EURODAC	Base de datos dactiloscópicos informatizada de la Unión Europea
EUROJUST	Unidad de Cooperación Judicial Europea
EUROPOL	Oficina Europea de Cooperación Policial
FBI	Federal Bureau of Investigation
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
GCHQ	Britain's Government Communications Headquarters
GDPR	General Data Protection Regulation 2016/679
GT29	Grupo de Trabajo del Artículo 29
IP	Internet Protocol
ISP	Internet Service Provider
JAI	Consejo de Justicia y Asuntos de Interior o Cooperación policial y judicial en materia penal
JAI	Justicia y Asuntos de Interior
LIBE	Comité de Libertades Civiles, Justicia y Asuntos de Interior de la Unión Europea
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
NSA	National Security Agency
N-SIS	National Schengen Information System
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OECE	Organización Europea de Cooperación Económica
OLAF	Oficina Europea de Lucha contra el Fraude
ONG	Organización no Gubernamental
ONU	Organización de las Naciones Unidas
PESC	Política Exterior y de Seguridad Común
PIDCP	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas
PNR	Passenger Name Records

REC	Recomendación
RGPD	Reglamento General de Protección de Datos (UE) 2016/679
SEPD	Supervisor Europeo de Protección de Datos
SIRENE	Supplementary Information Request at the National Entry
SIS	Sistema de Información Schengen
SIS II	Sistema de Información Schengen de segunda generación
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TCE	Tratado constitutivo de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TE-SAT	The European Union Terrorism Situation and Trend Report
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TTIP	Trasatlantic Trade and Investment Partnership
TUE	Tratado de la Unión Europea
UE	Unión Europea
UIP	Unidades de Información sobre Pasajeros
UK	United Kingdom
VIS	Visa Information System
WPISP	Working Party on Information Security and Privacy

INTRODUCCIÓN

La relación entre privacidad y seguridad en las sociedades avanzadas constituye, sin lugar a dudas, una de las cuestiones más complejas y polémicas que se plantea respecto a este ámbito en la actualidad, tanto por la amplitud y heterogeneidad de los posibles significados de ambos conceptos como por la dificultad inherente a tratar de encontrar un equilibrio entre los dos. Al describir el "binomio" –que no dicotomía– "privacidad y seguridad", es útil partir de una suposición; esta no es otra que la conexión íntima que existe entre estos valores sociales, tanto desde un punto de vista general como en el sistema normativo europeo en particular. La presentación de un "conflicto" ineludible entre el "derecho a la privacidad" y la "garantía de la seguridad", entre la satisfacción del derecho del individuo a la protección de su privacidad y la función de seguridad pública ejercida por el Estado es, de hecho, una simplificación que no tiene en cuenta el alcance de las posibles variaciones de las dos instituciones en juego. Es más, como se podrá comprobar a lo largo de la presente investigación, la protección de la privacidad como derecho individual, y la función de seguridad como un interés colectivo, no pueden reducirse a una de sus posibles manifestaciones. Por el contrario, y por lo que respecta a la protección de datos personales, ésta se define expresamente en el nuevo Reglamento General de Protección de Datos (UE) 2016/679, no sólo como un derecho individual, sino también como un interés público relevante para la sociedad, una garantía para la democracia y un elemento necesario para su buen funcionamiento. Por lo tanto, en el desarrollo de este trabajo se tratará de analizar los nuevos desafíos a la protección de la privacidad que se plantean en un nuevo escenario que exacerba la seguridad como consecuencia de los peligros y amenazas surgidos a escala global tales como el terrorismo, en busca de un posible equilibrio entre ambos términos en el que la acción protectora del Estado, a través de medidas cada vez más restrictivas, no haga que se limiten indebidamente los espacios de los derechos y libertades fundamentales propios de un Estado de Derecho.

Por lo tanto, y como primer elemento del binomio, esta investigación tiene que ver con la seguridad pública/nacional que, a pesar de la existencia de directrices internacionales, no ha sido definida de manera unívoca en la Unión Europea. Esta cuestión de la noción de seguridad pública es uno de los ámbitos que más atrae la atención de los constitucionalistas y administrativos en la actualidad y que, por razón de su importancia y complejidad, exigiría una investigación específica, por lo que se partirá de un concepto común y asentado para el desarrollo de esta tesis. En efecto, ni la legislación de la UE ni la jurisprudencia del Tribunal

de Justicia de la Unión Europea (en adelante, TJUE) definen este concepto, aunque el mismo Tribunal, como se podrá comprobar, ha declarado en ocasiones que "las excepciones a los derechos fundamentales deben interpretarse de manera restrictiva y justificada". Este criterio interpretativo debe tenerse en cuenta ya que la falta de una definición de lo que se entiende por "seguridad" afecta desde luego al ámbito de aplicación de normativa de la UE, donde se establece que la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro. Evidentemente, esto no significa que el Derecho de la Unión sea inaplicable a esta cuestión. Por el contrario, son las instituciones de la UE, y en particular el TJUE, las que tienen la facultad de evaluar la interpretación de las medidas de "seguridad" a nivel de los Estados miembros y la forma en que se implementan. La "seguridad", es una función, aunque en sus diferentes significados, caracterizada por una dimensión histórica, política y social que presenta una importante paradoja ya que es el fundamento del Estado de Derecho y garantiza el disfrute de los derechos fundamentales, pero igualmente, su ejercicio se basa en la limitación de derechos y libertades individuales con los que entra en tensión y que constituyen una última barrera a la misma. Esto es lo que explica que, en la actualidad, la privacidad, en particular la protección de datos personales, tenga un fuerte impacto en la política de seguridad interior dentro de la Unión Europea. La posibilidad de restringir y limitar los derechos fundamentales ha sido invocada en numerosas ocasiones en la lucha contra el terrorismo internacional, pero igualmente, estos derechos se han erigido como límite a las medidas de seguridad.

De hecho, la manera más efectiva de proteger a la democracia de los peligros que la acechan, implica la realización, sólo abstracta, de un equilibrio de intereses. El Estado está llamado a poner en una escala la necesidad de proteger la democracia de las amenazas de que se traten –entre otras, y principalmente, el terrorismo– y, por otro lado, la necesidad de garantizar la protección de los derechos humanos mediante su limitación por razones extraordinarias. Son mecanismos de toma de decisiones que operan en unas situaciones extremas en las que el conjunto de derechos y garantías, que cada uno de nosotros tiene en condiciones normales, está sujeto a limitaciones justificadas por la necesidad de alcanzar un objetivo común más elevado. En una situación de emergencia, como el que se determina en ocasiones por razón de una escalada de actos terroristas, los derechos individuales se someten al objetivo principal de garantizar la seguridad nacional. Teniendo en cuenta estas premisas, no puede sorprender que las primeras codificaciones de los derechos fundamentales pongan el derecho a la seguridad entre los derechos humanos innatos. Entre ellos cabe mencionar, la Declaración de los Derechos del Hombre y del Ciudadano de 1789 que en el artículo 2 afirma

perentoriamente que «*La finalidad de cualquier asociación política es la protección de los derechos naturales e imprescriptibles del Hombre. Tales derechos son la libertad, la propiedad, la seguridad y la resistencia a la opresión*». Para protegerse a sí mismo y garantizar su supervivencia, el Estado se ve obligado, paradójicamente, a forzar los principios constitucionales en los que se inspira todo el sistema de gobierno, para garantizar la preservación del orden democrático. No hace falta decir que una supresión de este alcance solo puede ser admitida en presencia de circunstancias seriamente excepcionales, que determinan un estado de necesidad que no deja lugar a ninguna solución alternativa; de lo contrario, la supervivencia del orden democrático establecido se pondría en peligro.

En este contexto, es el derecho a la privacidad el que más sufre, a día de hoy, una mayor tensión a nivel internacional, especialmente por lo que respecta a la relación entre la protección de los datos personales y las políticas implementadas por los Estados en la lucha contra el terrorismo. Una de las manifestaciones más intensas de esta incidencia sobre la privacidad tiene lugar como consecuencia de la enorme cantidad de datos personales generados y difundidos a través de nuevas tecnologías de comunicación e información, junto con la mayor capacidad para "conservarlos", "organizarlos" y "ordenarlos", que permite a los Estados obtener de los mismos nuevos datos, esto es, una información adicional que le permite construir un perfil muy preciso de individuos y grupos sociales. Perfilar significa reconstruir la identidad de los demás, conocer a una persona, sus hábitos, sus opiniones y sus deseos. Como es evidente, esta técnica resulta muy eficaz para el desarrollo de la función de seguridad por parte de las autoridades públicas en la prevención, detección y enjuiciamiento de delitos, aunque igualmente, la posibilidad de un conocimiento detallado de los ciudadanos incide gravemente en su privacidad.

Este desarrollo masivo por parte de las autoridades públicas de instrumentos que afectan a la privacidad de los ciudadanos ha tenido lugar a partir de los ataques terroristas del 11 de septiembre de 2001, que cambió la estrategia para combatir el terrorismo a través de la aplicación de una nueva metodología para la adquisición de datos indiscriminados a escala mundial. Si bien el terrorismo internacional ya existía, el atentado de las Torres Gemelas supuso un punto de inflexión histórico que llevó a los EE.UU. a la adopción generalizada de medidas que suponían un enorme sacrificio de la privacidad a partir de la "*Patriot Act*" de 2001, junto a otras medidas complementarias que igualmente afectan a las libertades constitucionales más tradicionales. Pero, desde el 11-S, desgraciadamente, se han sucedido otros grandes atentados en Europa como los de Madrid (2004), Londres (2005 y 2016), Niza

(2016), Berlín (2016), Barcelona (2017), entre otros, que no han hecho si no agravar algo que ya se había afianzado: un sentimiento de vulnerabilidad en los países occidentales, la sensación de una amenaza global y la necesidad de dar una respuesta supranacional al nuevo fenómeno terrorista.

La inseguridad es el elemento más común y característico de la situación geopolítica actual y es, precisamente, la sensación de peligro e inestabilidad la que sirve de base legitimadora a las medidas institucionales para la "lucha contra el terrorismo" basadas en la restricción de los derechos y libertades. En este sentido, es importante destacar cómo frente al peligro, la conciencia común se orienta hacia una instancia de protección y prevención que no es otra que los poderes públicos. La consecuencia directa de esta dinámica se encuentra al observar el impacto que la emergencia terrorista ejerce en la escala jerárquica de prioridades y valores compartidos en un Estado de derecho: la seguridad pública se eleva como valor prioritario, y se convierte en "un derecho de los ciudadanos y una obligación de los poderes públicos" que sirve de base a la tendencia a "comprimir las garantías de los derechos individuales".

Otra de las técnicas que viene a desequilibrar el binomio "privacidad y seguridad", es el problema de la vigilancia masiva por razones de seguridad nacional que se encuentra en el centro del debate internacional: el denominado "*Datagate*". Este hecho será abordado en diversos puntos de esta investigación, ya que tiene serias repercusiones sobre la evolución de la política relativa a la privacidad en Europa y ha generado importantes diferencias en las relaciones a nivel internacionales entre Europa y los EE.UU. El famoso escándalo de "*Datagate*", surgido a raíz de las revelaciones, en junio de 2013, por parte del Sr. Edward Snowden, analista de la CIA, tiene su origen en el uso de las normas introducidas en los Estados Unidos después del 11 de septiembre: la existencia de un programa de vigilancia masiva, llamado "*PRISM*", destinado a recabar datos personales de ciudadanos de todo el mundo –y por lo tanto también europeos– por parte de las autoridades federales de EE.UU. por razones de seguridad nacional, a través del acceso a los servidores de las muchas empresas tecnológicas ubicadas en territorio estadounidense. Este programa fue administrado, desde 2007, por la Agencia de Seguridad Nacional de EE.UU. (*National Security Agency - NSA*) con la participación de las principales compañías de servicios de Internet (incluidas Google, Microsoft, Yahoo!, Facebook, Apple, *etc*.).

Por lo tanto, el programa "*PRISM*" se implementó a través de un sistema que permitió la obtención de datos a gran escala con la consiguiente violación de las normas nacionales e

internacionales relativas a la protección de la privacidad. Según las revelaciones del Sr. Snowden, la *NSA*, con el fin de ampliar el área interceptada, realizó habitualmente ataques contra redes de Internet dirigidas a los enrutadores más importantes, tanto de países amigos (como los Estados europeos) como de proveedores de otros Estados (como China o Brasil). La base jurídica del programa "*PRISM*" se encuentra en la Sección 702 de la Ley de Vigilancia de la Inteligencia Extranjera (*Foreign Intelligence Surveillance Act - FISA*) de 1978 de EE.UU., modificada varias veces, entre otras, por la *Patriot Act* de 2001 por el entonces presidente Bush como resultado de los ataques de las Torres Gemelas y extendida por el presidente Obama en 2013.

Este cambio en la estrategia estadounidense después de los ataques de 2001, y el desarrollo de una política de interceptación y obtención indiscriminada de los datos personales a escala mundial de ciudadanos estadounidenses y extranjeros, fue confirmado también por el Sr. Bill Binney, un ex miembro de la *NSA*. Esto confirmó que la idea de un panóptico universal no era una mera quimera, sino que era una realidad ya que se permitía la interceptación legal en la vida privada de los ciudadanos, justificándolo en razones de seguridad para proteger mejor a la sociedad. Este escándalo de la vigilancia de masas también salpicó al Reino Unido, tal y como reveló el periódico *The Guardian*, ya que la agencia de espionaje británica, conocida por sus siglas en inglés *GCHQ*, estaba "pinchando" cables de fibra óptica que transportan comunicaciones electrónicas y compartía grandes cantidades de datos con la *NSA*, a través de un programa conocido como "*TEMPORA*".

La trascendencia de tales revelaciones, puso de manifiesto la existencia de un sistema de vigilancia con repercusiones en la vida privada de personas de todo el mundo, que no se limitaba a los secretos de Estado o comerciales, sino que sistemáticamente interceptaba, clasificaba y almacenaba las comunicaciones personales a gran escala. Se trata de una interferencia tanto en el respeto de la vida privada y familiar, como en el derecho a la privacidad y la protección de datos, ambos protegidos a nivel europeo por la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, Carta de Niza o CDFUE). Esa vigilancia masiva e indiferenciada, como se pondrá de manifiesto, es desproporcionada en su naturaleza y constituye una injerencia injustificada en los derechos garantizados por los artículos 7 y 8 de la Carta.

La vulneración de estos derechos fundamentales no puede quedar justificada ni siquiera por la intensificación de la amenaza terrorista como ha ocurrido en los últimos años en los que

los Estados europeos, han tenido que adoptar medidas de seguridad para frenar el terrorismo internacional. Es una reacción 'fisiológica' que los sistemas democráticos adopten medidas policiales extraordinarias "para hacer frente a las amenazas a la seguridad" de sus ciudadanos, especialmente si provienen del terrorismo. Sin embargo, tales medidas deben respetar los "principios de legalidad", "necesidad y proporcionalidad" y las normas internacionales para la protección de los derechos fundamentales. A esto se suma el hecho de que el avance tencológico en el ámbito de las comunicaciones digitales está debilitando progresivamente la protección de la privacidad de los ciudadanos y se permite crear nuevos sistemas de vigilancia con un alcance y un impacto cada vez mayor.

A la luz de los acontecimientos actuales, parece razonable creer que la tendencia, en los próximos años, será la de un fortalecimiento de las medidas de seguridad y un debilitamiento progresivo de las garantías para proteger el ámbito privado de los ciudadanos. Esta dinámica otorga una mayor importancia al debate en torno al valor que debe otorgarse a la privacidad, frente a la estrategia política generalizada que lleva a hacer prevalecer la "seguridad". Este planteamiento también se está asumiendo a nivel social por una gran parte de la población que verá en las tecnologías de la comunicación una herramienta de defensa a disposición de los gobiernos para defender a los ciudadanos de la amenaza terrorista. Por lo tanto, el problema pasa del nivel político al social, es decir, a la percepción de la amenaza real (como terrorismo) y del remedio ideal (recopilación de nuestros datos). Uno de los mayores riesgos que está teniendo lugar hoy, desde un punto de vista social, es la idea generalizada de que "en nombre de mi seguridad también puedo perder parte de mi libertad, así que no tengo nada que ocultar".

El segundo de los elementos que componen el binomio conceptual sobre el que se estructura la presente investigación es la privacidad, que está marcada por una particularidad fundamental: se trata, de hecho, de uno de los derechos más difíciles de definir, tal vez debido a la pluralidad intrínseca del contenido que lo caracteriza. Al trazar una especie de línea de evolución del derecho a la privacidad, o derecho a la intimidad –como se le conoce en la mayoría de los países de la Europa continental– es posible identificar, en primer lugar, una visión inicial de protección de la esfera privada del individuo concebido como el derecho "a ser dejado solo" y "a ser dejado en paz". Como es bien sabido, la primera teorización doctrinal unitaria del derecho a la privacidad se remonta a fines del siglo XIX con el derecho a la privacidad definido en un artículo bien conocido de 1890 de Warren y Brandeis "*The*

Right to Privacy"[1]; publicado en Harvard Law Review, los dos autores definieron la privacidad ("*right of privacy*") como "*right to be let alone*", derecho a ser dejado en paz.

El mérito histórico más evidente del trabajo de Warren y Brandeis es precisamente el intento de reconstruir el derecho a la privacidad como una cuestión legal autónoma, que ya no está exclusivamente vinculada al derecho de propiedad o que coincide con el derecho a la privacidad de las comunicaciones interpersonales. En la sociedad industrial, el anonimato urbano dio lugar al deseo de defender la intimidad privada contra la injerencia de los periódicos en la vida de las personas y, sobre todo, en la burguesía de la ciudad, como también emergió la necesidad de protegerse contra las intrusiones del gobierno en la esfera privada de los ciudadanos. El derecho a la privacidad se configuró entonces como un derecho de contenido negativo, como un interés en el secreto contra cualquier interferencia ajena dentro del hogar.

Con la llegada del Estado social y democrático, después de la Segunda Guerra Mundial, se superó la configuración individualista imperante del derecho a la privacidad. Los sistemas legales han sentido la necesidad de garantizar a los ciudadanos la no injerencia indebida (tanto de los organismos públicos como de otros sujetos privados) en la intimidad privada, excluyendo la difusión de datos, hechos e informaciones que puedan afectar a un individuo en el desarrollo de su área estrictamente privada y personal. El derecho a la privacidad no es sólo, por lo tanto, una libertad negativa en la que el Estado se abstiene de llevar a cabo acciones que pueden negar o limitar las libertades individuales, el derecho a la privacidad es un derecho funcional a la libre expresión de la persona. Así, hemos pasado de una concepción individualista del derecho a la privacidad a una concepción social, de la cual surge la necesidad de una disciplina jurídica que comprometa al Estado a favorecer la participación y el control de los sujetos involucrados.

El derecho al respeto de la vida privada y el derecho a la protección de datos personales, aunque estrechamente relacionados, son derechos distintos. La protección jurídica de la privacidad en Europa ha experimentado una evolución regulatoria progresiva que involucra la fuente constitucional, el marco regulatorio interno, europeo e internacional, y, finalmente, la jurisprudencia constitucional, europea y ordinaria. El derecho a la privacidad, mencionado en la legislación europea como el derecho al respeto a la vida privada, aparece en el derecho

[1] Samuel D. WARREN, Louis D. BRANDEIS (1890), «The Right to Privacy», en *Harvard Law Review*, vol. 4, N. 5 (Dec. 15), págs. 193-220.

internacional, en la Declaración Universal de Derechos Humanos, adoptada en 1948, como uno de los derechos humanos fundamentales protegidos. Poco después de la adopción de la Declaración, Europa también afirmó este derecho en el Convenio Europeo de Derechos Humanos adoptado en 1950. El Convenio establece que "todos tienen derecho al respeto por su vida privada y familiar, su hogar y su correspondencia". Se prohíbe la interferencia con este derecho por parte de una autoridad pública, excepto cuando la interferencia esté de acuerdo con la ley, persiga intereses públicos importantes y legítimos y sea necesaria en una sociedad democrática.

Estos dos textos normativos se adoptaron mucho antes del desarrollo de los ordenadores y de Internet y del surgimiento de la sociedad de la información, presentando nuevos riesgos para el derecho al respeto de la vida privada relacionados con los nuevos métodos y formas de obtención y tratamiento de la información. Esta es una tendencia determinada por fenómenos interdependientes, como los nuevos métodos de recopilación automatizada de datos mediante el uso de la tecnología de la información, y la necesidad cada vez mayor de datos para la adopción de decisiones por parte de instituciones públicas y privadas: una gran cantidad de datos relacionados con la vida, la esfera privada, la salud, el pensamiento político, la creencia religiosa de un individuo que, conectados entre sí, pueden elaborar el perfil de un individuo. La privacidad se separa así del individuo físico para extenderse a la información y los datos a los que este individuo se refiere y que ofrecen una representación.

Por lo tanto, pasamos a definir la privacidad también sobre la base de los contenidos informativos del individuo, y sobre la necesidad de defenderla de los múltiples casos en los que sería posible configurar un control sobre los ciudadanos a través de sus datos personales. Por esta razón, hemos pasado del "derecho a la privacidad" como garantía ofrecida por la legislación al "derecho a la protección de datos personales", creando así un nuevo derecho, capaz de proteger los flujos de información relacionados con los datos personales en todos los sectores públicos y privados, extendiendo el concepto de privacidad en términos más amplios. En el ordenamiento jurídico de la UE, la "protección de datos" se reconoce como un "derecho fundamental", separado del "derecho fundamental al respeto de la vida privada". Un segundo elemento que debe tenerse en cuenta es la necesidad de adoptar un enfoque multidisciplinar sobre la cuestión de la privacidad. De hecho, la interconexión entre los componentes jurídicos, políticos, económicos, informáticos y sociológicos es tan estrecha que es muy difícil aislar los temas individuales o centrar la atención cuando se

refieren a cuestiones relacionadas con los derechos humanos, así como para tener en cuenta los nuevos comportamientos llevados por la sociedad digital.

En este contexto se plantea la presente investigación que, dentro del análisis de la relación entre las medidas de seguridad y las garantías de libertades fundamentales, centra su objeto en identificar las trayectorias futuras del derecho a la privacidad, analizando la relación con la seguridad pública y cómo está transformando el derecho fundamental a la privacidad en el contexto de la Unión Europea, a partir del sistema de protección internacional actual. Por lo tanto, el estudio se centra, en particular, en el binomio "privacidad y seguridad" que, hasta hoy, ha caracterizado la visión dominante y que no se ha llegado a superar, planteándose la integración de los dos principios que lo componen.

Brevemente delineada la naturaleza del derecho a la privacidad en su evolución internacional, es necesario concentrarse en el contenido del derecho mismo para el propósito de este trabajo, ya que también ha sido objeto de una transformación significativa durante los años. A partir de este planteamiento inicial la investigación se centra en identificar el equilibrio que se ha mantenido entre la protección de la privacidad y la garantía de la seguridad pública en el nacimiento y primera evolución de la normativa sobre protección de datos en Europa. El trabajo continúa centrándose en la evolución de este equilibrio a través de la jurisprudencia del TJUE hasta llegar a la aprobación del nuevo "paquete de reformas" de protección de datos que establece un nuevo marco a partir del cual se replantea esta relación entre protección de datos y seguridad en su proyección hacia el futuro inmediato.

De manera más detallada, la investigación comienza analizando el encaje del derecho a la privacidad dentro del ámbito de las normas internacionales de protección de los derechos humanos (**Capítulo I**). A nivel universal, entre las más importantes, se encuentra tanto la Declaración Universal de Derechos Humanos de 1948 (artículo 12) como el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17) que establecen el derecho de cada persona a no ser «*objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación*». La creciente importancia de la privacidad queda también demostrada por la acción de las Naciones Unidas que, a partir de 2013, adoptó una serie de resoluciones sobre el denominado "*The Right to Privacy in the Digital Age*" ("El derecho a la privacidad en la era digital"). Particularmente importante, a pesar de su naturaleza de *soft law*, han sido las "Directrices sobre protección de la privacidad y flujos transfronterizos de datos" adoptadas por la

Organización para la Cooperación y el Desarrollo Económico (en adelante, OCDE) en 1980 (revisadas en 2013), que "tuvieron el mérito de declarar ciertos principios que habrían sido puntos de referencia reales para las normas y procedimientos posteriores, aún vigentes, con respecto al tratamiento y la circulación transfronteriza de datos personales".

También en el marco del Consejo de Europa (en adelante, CdE), el derecho a la privacidad ha encontrado su lugar gracias a la contribución del Tribunal Europeo de Derechos Humanos (en adelante, TEDH) que lo ha hecho parte de la protección en el ámbito del "derecho al respeto a la vida privada y familiar", establecido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 (en adelante, CEDH), que consagra el derecho al respeto de la vida privada y familiar: «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*». Los jueces del TEDH son de los primeros que han abordado la necesidad de garantizar el derecho a controlar la información que deja la esfera privada del individuo. Además, el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 (Convenio n. 108) (en adelante, Convenio n. 108), fue el primer instrumento internacional jurídicamente vinculante adoptado por una organización internacional en el ámbito de la protección de datos, formulando una primera definición de protección de datos, como un derecho garantizado a cualquier persona al «*respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona*» (artículo 1 del Convenio n. 108).

En las sentencias examinadas en la investigación se puede comprobar como los jueces del TEDH fueron los precursores al declarar que la mera conservación de datos relativos a la vida privada de un individuo equivale a una injerencia sistemática en el sentido del artículo 8 del CEDH. A este respecto, es irrelevante si la información almacenada es, entonces, realmente usada o no. Sin embargo, al determinar si la información personal conservada por las autoridades involucra alguno de los aspectos de la vida privada mencionados anteriormente, la Corte tendrá debidamente en cuenta el contexto específico en el que se ha registrado y conservado la información en cuestión, la naturaleza de los datos obtenidos, la forma en que se usan y procesan estos datos y los resultados que se pueden obtener de ellos.

También estos jueces del TEDH subrayan en su jurisprudencia que la protección de los datos personales es fundamental para que una persona pueda disfrutar de su derecho al respeto de

la vida privada y familiar, tal como lo garantiza el artículo 8 del CEDH. La legislación nacional debe ofrecer salvaguardias adecuadas para evitar cualquier uso de datos personales que pueda ser incompatible con las garantías de este artículo. La necesidad de tales salvaguardias es aún mayor cuando se trata de la protección de los datos personales sometidos a un tratamiento automatizado, especialmente cuando dichos datos se utilizan con fines policiales. La legislación nacional debe garantizar especialmente no sólo que dichos datos "sean pertinentes y no excesivos en relación con los fines para los que se almacenan", sino también que se conserven "en una forma que permita la identificación de los interesados" por un período "no superior a lo estrictamente necesario" según los fines para los que fueron almacenados. También debe prever las garantías adecuadas de que los datos personales almacenados sean protegidos de manera eficaz contra el uso indebido y el abuso.

La investigación continúa con el análisis de la protección de los datos personales y el respeto por la vida privada como derechos fundamentales en lo que se refiere a sus límites y perspectivas en las normativas europeas más destacadas (**Capítulo II**) que siempre han insistido en "la necesidad de lograr un equilibrio" que combine "el refuerzo de la seguridad" con la "protección de los derechos humanos, incluida la protección de los datos personales y la privacidad". El conjunto de normas sobre privacidad en la UE es el resultado de un proceso regulatorio que comenzó a mitad de los años noventa. Antes de la entrada en vigor del Tratado de Lisboa en 2009, la legislación sobre protección de datos personales en el Espacio de Libertad, Seguridad y Justicia (en adelante, ELSJ) se dividía entre el primer pilar (protección de datos para fines privados y comerciales, con método de integración comunitario) y el tercer pilar (protección de datos para fines de orden público, con toma de decisiones según el método de cooperación intergubernamental).

También el proceso de toma de decisiones siguió dos conjuntos diferentes de normas. Como consecuencia, entre los que figuran instrumentos pertenecientes al antiguo primer pilar, estaba en vigor la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (derogada en mayo de 2018), que estableció, por primera vez, un marco regulador con el objetivo de «*establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión*»[2]. Tras su adopción, la UE ha regulado cuestiones

[2] «Protección de los datos personales», en *EUR-Lex*. Disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:31995L0046 [consulta: 18 de junio de 2019].

importantes de protección de datos, incluidas, en relación con el tema de nuestro análisis, la protección de los datos personales tratados en el contexto de la cooperación policial y judicial en materia penal. La Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal reguló la protección de datos en el antiguo tercer pilar. Se trataba de un sector no cubierto por la Directiva 95/46/CE, que se refería al tratamiento de datos personales en el antiguo primer pilar. La Decisión Marco, por lo tanto, solo se centraba en los datos judiciales y policiales intercambiados entre los Estados miembros y las autoridades y sistemas de la UE y no abarcaba los datos nacionales.

La estructura de pilares desapareció con el Tratado de Lisboa, que proporciona una base más sólida para el desarrollo de un sistema de protección de datos más claro y eficaz, y al mismo tiempo concede nuevas competencias al Parlamento Europeo, que asume el papel de colegislador. De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE), que establece que «*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*», el Parlamento y el Consejo establecen normas relativas a la protección de las personas físicas con respecto al tratamiento de datos personales por parte de «*las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos*» (apartado 2).

La novedad principal y específica de la CDFUE, que se convirtió en vinculante con la entrada en vigor del Tratado de Lisboa, radica precisamente en la evolución y especificación de la protección de la privacidad en la protección de los datos personales. La Carta establece dos formas distintas de protección de la privacidad y datos personales, respectivamente a los artículos 7 ("Respeto de la vida privada y familiar") y 8 ("Protección de datos de carácter personal"). Este último artículo, de hecho, establece que «*toda persona tiene derecho a la protección de los datos personales que le conciernan*»; los datos deben tratarse de acuerdo con el principio de lealtad, para «*fines concretos y sobre la base del consentimiento de la persona*» interesada u otra base legítima requerida por la ley.

Asimismo, se reconoce el derecho a tener "acceso a los datos" que le conciernen y que se han almacenado, así como a un derecho de rectificación. Por lo tanto, la protección de los datos personales como un derecho fundamental está protegida por separado del derecho a la

vida familiar (que la Carta de Niza establece en el artículo 7). El derecho a la protección de datos también se establece en el derecho primario y secundario de la UE, que garantiza, en sus respectivos campos de aplicación, que "el tratamiento de datos personales se lleva a cabo de manera lícita" y sólo en la medida necesaria para lograr el objetivo legítimamente perseguido. Estos derechos se extienden a todas las personas, ya sean ciudadanos de la UE o terceros países. De conformidad con el artículo 52, apartado 1, de la Carta, «*cualquier limitación*» al ejercicio de estos derechos debe ser necesaria y proporcionada, responder eficazmente a los «*objetivos de interés general reconocidos por la Unión*», estar prevista «*por la ley y respetar el contenido esencial*» de los mismos «*derechos*». Además, teniendo en consideración que en la Directiva 95/46/CE la protección de datos era, en última instancia, funcional para la consecución de objetivos económicos subyacentes al ordenamiento jurídico comunitario, la "revolución" de la Carta de Niza reside en la protección del derecho en sí mismo y por sí mismo.

A primera vista, esto parece un marco legal sin duda significativo y en cierta medida impresionante. Sin embargo, la experiencia muestra que en los últimos años este marco ha sido superado por los rápidos desarrollos tecnológicos y necesita una mejora urgente para proporcionar una mayor protección de los derechos individuales. Esto es, de hecho, un proceso contínuo que implica una revisión general de la legislación de la UE. Sin embargo, las propias instituciones europeas abordaron este escenario de incertidumbre regulatoria a través de la propuesta de reforma de todo el paquete normativo de datos personales de la UE elaborado por el Parlamento Europeo y el Consejo en 2012, que será analizado en un capítulo posterior. Aunque ha habido un proceso de fortalecimiento del nivel de protección de la privacidad con la entrada en vigor del Tratado de Lisboa (artículo 16 del TFUE), aún surgen muchas dudas con respecto a la aplicación de las garantías previstas por el sistema jurídico europeo a la luz de algunas contradicciones obvias. De hecho, la tendencia del TFUE y del TUE fue no considerar la cuestión del tratamiento de datos como un tema unitario y general, sino como un área muy especial sujeta a la aplicación de disposiciones diversificadas y no uniformes.

Después de los atentados terroristas del 11-S de 2001, también en Europa se propició una extensión progresiva del uso de los datos de personas que llegaban de terceros países a territorio europeo para fines policiales. Estas informaciones personales, originalmente sólo previstas para controlar la inmigración, se recogieron en sistemas de información para la gestión de la información del Espacio Europeo de Libertad, Seguridad y Justicia y la

protección de datos (**Capítulo III**) tales como el Sistema de Información Schengen (SIS), Eurodac, el Sistema de Información de Visados (VIS), Decisión Prüm y Europol. La elección de estos sistemas en detrimento de otros está motivada por el hecho de que éstos han sido reformados en los últimos años en sus respectivas legislaciones para permitir "el acceso a las autoridades policiales de los Estados miembros" y a Europol, con los consiguientes riesgos para la protección de la privacidad. Por esta razón, en este trabajo se pone de manifiesto el posible conflicto que se deriva de estas prácticas con el derecho fundamental de protección de datos en la UE. Para ello, se examina si los sistemas a través de los cuales la UE "ha ido ampliando de manera gradual el uso de información personal para finalidades policiales" pueden estar vulnerando los principios de necesidad y limitación de finalidad como parte del derecho de protección de datos de la UE.

Como consecuencia de las diversas actuaciones extraordinarias de seguridad en Europa desarrolladas en la última década, ha surgido la "necesidad de una mayor cooperación entre las autoridades nacionales" de los diferentes Estados para hacer un uso común más sistemático de los datos "para luchar contra el terrorismo y otros delitos". El clima de tensión causado después de los ataques terroristas ha incentivado la adopción de actos particularmente perjudiciales para el derecho a la privacidad por parte del legislador comunitario. En ese sentido, el TJUE ha tenido, y tiene, un papel importante: se erige como baluarte a la protección de la privacidad de los ciudadanos europeos (**Capítulo IV**). Como se ha explicado, entre las normativas europeas que afectan a los derechos de la privacidad en Europa está la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que fue un claro ejemplo. La adopción de esta Directiva, de hecho, se orienta a crear un sistema enorme y desproporcionado de vigilancia de masas justificado por la lucha contra el terrorismo. Sin embargo, esta Directiva ha demostrado a lo largo de los años su inadecuación y sus efectos negativos sobre el derecho a la protección de los datos personales. De hecho, la Directiva era incompatible con las normas europeas que subyacen a la protección de la privacidad y los datos personales y, en particular, con los artículos 7, 8 y 52, apartado 1, de la CDFUE. Por lo tanto, es importante que el TJUE (Gran Sala), en su sentencia de 8 de abril de 2014 (el llamado caso *Digital Rights Ireland*), haya declarado finalmente, refiriéndose a los artículos antes mencionados de la Carta, la invalidez de la Directiva 2006/24/CE sobre la conservación de datos de tráfico telefónico y telemático. De hecho, este fallo resulta esencial en tanto que recupera un equilibrio entre la seguridad y la

privacidad. Un equilibrio que es esencial para hacer valer los derechos fundamentales en el espacio público europeo.

El fallo ha tenido también consecuencias sobre otras cuestiones sensibles, relativas en concreto a la "elaboración de perfiles" y la cooperación transfronteriza en la lucha contra el terrorismo y la delincuencia transfronteriza. Tras los atentados terroristas de 2015 en París y las "nuevas preocupaciones" sobre posibles amenazas al sistema de seguridad interior de la UE planteadas por los "combatientes extranjeros" ("*foreign fighters*"), se desbloqueó con gran rapidez un asunto que llevaba encallado desde 2011 y los ministros del interior acordaron rápidamente la aprobación y aplicación del registro de nombres de los pasajeros (*PNR*, por su sigla en inglés), también en los vuelos intracomunitarios.

En diciembre de 2015, el Parlamento Europeo y el Consejo llegaron a una solución de compromiso sobre este delicado tema con la adopción de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (*PNR*) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. Esta medida, en relación con el equilibrio entre las necesidades de seguridad y el respeto de los derechos fundamentales, como el derecho al respeto de la vida privada y el derecho a la protección de los datos personales, genera dudas sobre su proporcionalidad y su respeto de los derechos fundamentales. Otra cuestión de importancia crucial es el Acuerdo entre la Unión y los EE.UU. sobre el tratamiento y la transmisión de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

En este Capítulo cuarto, se podrá comprobar en las intervenciones jurisprudenciales del TJUE cómo ha evolucionado el derecho a la privacidad y se ha "afirmado de manera muy decisiva, en un diálogo constante entre el legislador y los tribunales que ha permitido ampliar el alcance del derecho a la privacidad", incluso en el contexto de serios desafíos terroristas. Teniendo esto en cuenta, además de la sentencia *Digital Rights Ireland*, el TJUE ha emitido en los últimos años algunas sentencias con un impacto significativo en las políticas de seguridad implementadas hasta el momento.

En este sentido, asimismo, destacan otros dos pronunciamientos a los que se hará referencia. En la línea de "proteger la trasferencia de datos de los ciudadanos europeos", en su sentencia

de 6 de octubre de 2015, en el asunto llamado *Schrems* o *Facebook*, el TJUE consideró que, al adoptar la Decisión 2000/520/CE, la Comisión Europea excedió los límites de la competencia que le atribuye el artículo 25, apartado 6, de la Directiva 95/46/CE, interpretado a la luz de la CDFUE, y declaró inválido dicho precepto. Con esta sentencia el Tribunal invalida todo el mecanismo de "Puerto Seguro" (en inglés, "*Safe Harbour*") que, basándose en un Acuerdo entre Comisión Europea y gobierno de Estados Unidos (Decisión 2000/520/CE), permitió la transferencia de los datos personales de los ciudadanos europeos para ser procesados por empresas y multinacionales de los EE.UU.

La normativa europea de protección de datos sólo permite "transferir datos a países que cuenten con un nivel adecuado de seguridad", premisa que, según el Tribunal, no cumplía EE.UU. Para el TJUE, el Acuerdo permitía que prevaleciera la seguridad nacional o el interés público de EE.UU. sobre los derechos fundamentales a la intimidad y la protección de datos, sin permitir que los ciudadanos tuviesen mecanismos para proteger con efectividad esos derechos. Además, el Acuerdo no ofrecía a los Estados miembros un margen suficiente para suspender las transferencias en caso de que apreciasen una vulneración de los derechos de los ciudadanos europeos.

La decisión del Tribunal, que nace de las consecuencias del mencionado caso "*Datagate*", ha tenido repercusiones importantes también en las relaciones comerciales y políticas entre Europa y EE.UU., tanto que se pusieron en marcha las nuevas negociaciones diplomáticas para llegar a una nueva versión del Acuerdo para la transferencia de datos personales de ciudadanos europeos a los Estados Unidos. El nuevo Acuerdo, llamado "Escudo de la privacidad UE-EE.UU." (en inglés, "*Privacy Shield*") fue adoptado por la Comisión Europea el 12 de julio de 2016, en sustitución del anterior "Puerto Seguro", a "fin de permitir los flujos de datos personales transatlánticos desde la Unión Europea hacia los EE.UU. garantizando, no solamente, un nivel de protección adecuado de los derechos de los ciudadanos europeos, sino también, mecanismos y recursos eficaces a favor de la seguridad jurídica". A estos efectos se evaluará si el nuevo "*Privacy Shield*" cumple con los requisitos establecidos por el TJUE que, en su sentencia de octubre de 2015, declaró inválido el antiguo marco "*Safe Harbor*". Asimismo, aun celebrando los esfuerzos para conseguir mejoras sustanciales en el "Escudo de la privacidad", en relación con la Decisión sobre "Puerto Seguro", a la que reemplazaba, formularemos algunas críticas y límites. Al tiempo, se analizará la ratificación de un acuerdo marco jurídicamente vinculante con los EE.UU. sobre

el intercambio de información y la protección de datos, conocido como el "Acuerdo Marco" (en inglés, "*Umbrella Agreement*").

Entre los objetivos de este Acuerdo es garantizar un alto grado de protección de los datos personales transferidos en el contexto de la «*cooperación transatlántica en la lucha contra el terrorismo y la delincuencia organizada*»[3]. En este sentido, los nuevos acuerdos intentan garantizar estándares elevados de protección y ayudar a "restaurar la confianza" tras las revelaciones de Edward Snowden, que, como se ha indicado, reveló la existencia de sistemas de vigilancia masiva de comunicaciones electrónicas de ciudadanos estadounidenses y europeos por parte de la *NSA*.

En los asuntos acumulados *Tele2 Sverige AB contra Post-och telestyrelsen* (C-203/15) y *Secretary of State for the Home Department contra Watson y otros* (C- 698/15) de 21 de diciembre de 2016, el TJUE dio una nueva indicación con respecto a las restricciones que la legislación de los Estados miembros debe imponer para el acceso a los datos conservados con el fin de cumplir con la CDFUE, continuando y profundizando las sentencias *Digital Rights Ireland* y *Schrems*. En la sentencia, el referido órgano jurisdiccional ha afirmado, que el derecho de la Unión prohíbe que un Estado miembro apruebe una normativa que obligue la "conservación generalizada e indiferenciada de los datos" tratados por el proveedor de servicios. La Corte de Luxemburgo rehusó una relectura respecto a las políticas de seguridad en el marco de las normas de los Tratados, incluyendo las de la CDFUE, incluso después de los recientes atentados. En síntesis, reitera que no se adecúa a criterios de proporcionalidad la conservación de todos los datos, sin tener en cuenta los riesgos que resulten de personas o situaciones determinadas.

De la reafirmación perentoria de la centralidad de los artículos 7 y 8 de la CDFUE con las tres sentencias que acabamos de mencionar, se deriva la posibilidad de identificar un núcleo fuerte de derechos fundamentales inviolables a nivel europeo, que sin duda incluye la protección de la vida privada y el contenido de la información de las personas. En este punto, nos centraremos en el análisis del proceso de aprobación de la reforma de protección de datos en la UE y las características principales de ambos actos legislativos (Reglamento y Directiva, de aplicación desde mayo de 2018) (**Capítulo V**), siempre insistiendo «*en la*

[3] Kristiina MILT (2019), «La protección de los datos personales», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo.

necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la protección de la vida privada y de los datos personales»[4].

La reforma, resultado de una larga negociación entre las distintas partes interesadas, representa un compromiso entre las diversas necesidades del uso de los datos en la sociedad de la información, lo que ha llevado al legislador europeo a dejar varias preguntas abiertas dirigidas a soluciones que se adoptarán a nivel nacional. En este contexto, los legisladores y las autoridades garantes han asumido y asumirán aún más en un futuro próximo un papel decisivo en la configuración del marco europeo común para el procesamiento de datos.
En particular, el 25 de enero de 2012, la Comisión presentó un paquete legislativo global para reformar la legislación de protección de datos de la UE justificado por el progreso tecnológico y la globalización y la falta de aplicación homogénea de la legislación de 1995 de manera uniforme por parte de los Estados miembros. En diciembre de 2015, el Parlamento Europeo y el Consejo llegaron a un acuerdo sobre las nuevas normas de protección de datos, después de casi tres años de largas negociaciones. En abril de 2016, se publicaron las nuevas normas que entraron en vigor en mayo de 2018. Las nuevas normas de protección de datos son el pacto final resultante de la convergencia de múltiples tensiones políticas entre filosofías e intereses en el que han confluido grupos de presión de manera incesante y feroz, como probablemente no se ha producido en la tramitación de ninguna otra normativa europea hasta la fecha. Es difícil encontrar una norma de la Unión Europea que haya recibido tanta presión de los lobbies y tantas enmiendas. Como se deduce del largo proceso de elaboración que precedió su aprobación el 14 de abril de 2016.

El nuevo "paquete de reformas" de protección de datos consiste en un Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante, RGPD), y de una Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[4] Kristiina MILT (2019).

El RGPD, que deroga la Directiva 95/46/CE, define los derechos de las personas físicas y establece las "obligaciones de los responsables y los encargados del tratamiento de datos". El Reglamento marca la apertura de "una nueva fase en la regulación de la protección de datos personales". Se establece un nuevo paradigma que tiene sus raíces en la Directiva 95/46/CE y, al mismo tiempo, intenta superar los límites que se han demostrado en los últimos años, como consecuencia de la aparición de nuevas formas de tratamiento de la información y una dimensión cada vez más colectiva del uso de la información. En este sentido el RGPD, en su décimo considerando, reconoce que «*para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea*».

Por lo tanto, no podemos dejar de apreciar el avance realizado con la aprobación del Reglamento que refleja el reciente proceso de evolución de la protección de datos personales y establece, entre lo que más interesa a la presente investigación: (1) la obligación de obtener un consentimiento explícito al tratamiento de datos; (2) limitaciones al tratamiento automatizado de datos; (3) el derecho de rectificación; (4) la obligación de los responsables del tratamiento de datos de proporcionar a las partes interesadas información transparente y de fácil acceso sobre sus datos personales; *etc*.

Al tiempo, el RGPD parece tener un régimen más garantista para los derechos de los ciudadanos europeos con respecto a la transferencia de datos personales a terceros países y organizaciones internacionales. Este es particularmente importante con respecto a la cuestión del equilibrio entre privacidad y seguridad, como veremos más adelante, especialmente con referencia a los datos transferidos a los EE.UU. Al mismo modo, es importante remarcar la no aplicabilidad del Reglamento (artículo 2) «*al tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión*», como «*por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención*».

El mismo Reglamento, en el considerando 16, «*tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión*». Respecto al tratamiento de datos personales, los Estados miembros pueden imponer restricciones, en condiciones específicas conforme al Derecho de la Unión, de las determinadas obligaciones y de los derechos siempre que dichas limitaciones sean medidas necesarias y proporcionadas en «*una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención* (…)*, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica*» (considerando 19). Estas limitaciones, plantean «*nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal*» (considerando 101). El RGPD es una norma que no tiene, a nuestro juicio, consenso unánime sobre una multiplicidad de conceptos lo que provoca que nos encontremos con una norma paradójica, incompleta, imprecisa en muchos puntos.

Con respecto a la Directiva (UE) 2016/680, las disposiciones que figuran en ella se aplican, en general, a todo el tratamiento de datos personales realizado en un Estado miembro para fines "institucionales"; es decir el «*tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública* (…) *y la libre circulación de dichos datos*» (considerandos 11 y 34). Se trata de un cambio significativo en comparación con la norma anterior en vigor (la Decisión Marco 2008/977/JAI del Consejo), que regulaba exclusivamente el intercambio de datos entre las autoridades competentes de los Estados miembros y el tratamiento posterior de los datos intercambiados en este contexto. La nueva Directiva en cuestión viene a afirmar el cambio producido operado tras el Tratado de Lisboa con la introducción de la protección de datos personales en el ámbito de la cooperación judicial y policial, como de corregir los importantes errores que tenía la Decisión Marco 2008/977/JAI.

La Directiva (UE) 2016/680 establece, en su considerando 93, que los Estados miembros deberán «*proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de sus datos personales y garantizar el libre*

intercambio de datos personales por parte de las autoridades competentes en la Unión», no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Entre dichas autoridades competentes «*se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad*» y «*también cualquier otro organismo o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas*» (considerando 11).

La utilización y la circulación de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, pueden incrementar la vulnerabilidad de los derechos de la persona, entre ellos el derecho a la protección de datos personales, lo que justifica la adopción de normas específicas encaminadas a regular los principios y derechos sobre protección de datos. A ello intenta responder la Directiva (UE) 2016/680, instrumento que va a contribuir, sin duda alguna, a sustentar el equilibrio entre la eficacia de las investigaciones y los procesos penales, por un lado, y los derechos de los sospechosos y acusados, incluido su derecho a la protección de datos, por otro. Aunque la Directiva introduce mejoras respecto a la legislación actual – como el hecho de que cubra transferencias de datos puramente internas, un mayor papel del Parlamento Europeo y la posibilidad de revisión por parte del TJUE –, éstas se han considerado insuficientes por gran parte de los expertos en el sector de la privacidad. El mayor descontento que ha provocado la Directiva tiene que ver con el limitado alcance del instrumento. Por ejemplo, la Directiva excluye datos tratados por agencias de la UE como Europol (y Eurojust), datos recogidos por el SIS, así como datos almacenados por compañías privadas y posteriormente utilizadas por entidades policiales.

En definitiva, y para concluir, en esta investigación se intentará trazar los nuevos desafíos a la protección de la privacidad, y por supuesto de los datos personales, que se colocan en el nuevo escenario abierto de los recientes ataques terroristas, en busca de un posible equilibrio entre las diferentes necesidades que permita no comprimir aún más los espacios de los derechos fundamentales, a pesar de las tendencias restrictivas. El trabajo que se lleva a cabo es un estudio que aborda desde la normativa internacional hasta la regional para proteger el derecho a la privacidad y el derecho a la protección de los datos personales, examinando su contenido, y poniendo de relieve las críticas y debilidades estructurales. Tales faltas han permitido a las autoridades públicas actuar al margen, en ocasiones, de los parámetros legales apropiados y específicos, contribuyendo decisivamente a facilitar una restricción

injustificada, no necesaria y desproporcionada, de estos derechos, en nombre de la lucha contra el terrorismo internacional.

El análisis de la legislación europea pertinente y el examen de las cuestiones derivadas de la adopción de decisiones por parte de las instituciones europeas en el ámbito de las medidas de lucha contra el terrorismo, nos llevan a considerar que las restricciones o violaciones del derecho a la privacidad y el derecho a la protección de los datos personales en estas áreas tienen su origen no sólo en las actividades invasivas de los poderes públicos para mantener un alto nivel de seguridad, sino también en la incapacidad de la legislación europea (y nacional) actual para proteger adecuadamente la privacidad y los datos personales.

Así pues, el futuro de la privacidad dependerá, principalmente, del cumplimiento de la normativa vigente, especialmente con respecto a los métodos de obtención y tratamiento de datos, y de la redefinición de las políticas de seguridad. En este sentido, la Unión debería «*garantizar la aplicación sistemática del derecho fundamental a la protección de datos, consagrado en la CDFUE*»[5], e invitar a los Estados a una redefinición de las estrategias para combatir el terrorismo internacional, poniendo como prioridad el cambio en los métodos de obtención y tratamiento de datos personales, la identificación de una metodología de investigación basada en la definición de un objetivo de sujetos (y datos relacionados) para ser sometidos a vigilancia, la cooperación entre los Estados en el campo de la inteligencia y, finalmente, la implementación de políticas de sensibilización, capaces de aumentar el grado de conocimiento y conciencia de los ciudadanos europeos en la materia de privacidad.

En este sentido, la presente tesis doctoral aspira a demostrar cómo, en una sociedad caracterizada por un rápido cambio tecnológico como la nuestra, sigue siendo «*necesario reforzar la posición de la UE sobre la protección de los datos personales*»[6] en todas las políticas de la Unión, incluida la lucha contra la prevención del delito de terrorismo y en las relaciones internacionales, y, muy en particular, con los Estados Unidos.

[5] Kristiina MILT (2019).
[6] Kristiina MILT (2019).

CAPÍTULO I

ALCANCE Y LIMITACIONES DE LA PROTECCIÓN JURÍDICA A LA PRIVACIDAD EN LA ESCENA INTERNACIONAL

1. El derecho al respeto de la vida privada y el derecho a la protección de datos personales en el marco legal internacional: una breve introducción

1. En este capítulo analizaremos las fuentes y la protección jurídica del derecho a la privacidad en el derecho internacional. Comenzamos explicando la protección en el marco internacional y, posteriormente, las normativas del Consejo de Europa, incluida la jurisprudencia del Tribunal Europeo de Derechos Humanos, que establecen normas mínimas. Observamos que los instrumentos internacionales mencionados han dotado al derecho de la privacidad de una protección global. Es por ello por lo que este capítulo recoge los instrumentos legislativos vigentes en materia, relacionados con el difícil equilibrio entre privacidad y seguridad pública, tanto a nivel internacional como del Consejo de Europa.

2. A nivel internacional la privacidad aparece en el artículo 12 de la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, «*estableciendo un límite a las injerencias arbitrarias en la vida privada, la familia, el domicilio o la correspondencia de las personas. El sentido de estas palabras, con relación al derecho de protección de datos personales, resulta evidente, ya que las intrusiones en la vida privada de las personas se pueden realizar a través de los modernos mecanismos de tratamiento automático de la información*»[7]. Destacamos otros instrumentos internacionales que también protegen dicho derecho. En primer lugar, el Pacto Internacional de los Derechos Civiles y Políticos, cuyo artículo 17 otorga un concepto de privacidad en términos idénticos al Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950. El Convenio es un tratado que es jurídicamente vinculante para sus Partes Contratantes y establece que "todos tienen derecho al respeto por su vida privada y familiar, su hogar y su correspondencia". Se prohíbe la interferencia con este derecho por parte de una autoridad pública, excepto cuando la interferencia esté de acuerdo con la ley, persiga intereses públicos importantes y legítimos y sea necesaria en una sociedad democrática.

[7] Carlos Eduardo SALTOR (2013), *La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación Argentina*, Tesis Doctoral, Madrid, Universidad Complutense de Madrid Facultad de Derecho, págs. 99.

3. «*Sin embargo, en defensa de la persona, y del libre ejercicio de sus derechos frente al progresivo desarrollo de los medios informáticos de tratamiento de la información, pronto resultan ineficaces los instrumentos jurídicos de defensa que hasta ese momento le son reconocidos con carácter general al individuo. Es decir, que los medios de defensa y prevención de injerencias en la intimidad y vida privada no eran suficientes para la protección de la persona frente a las intromisiones procedentes de una utilización abusiva o ilegítima con la informática*»[8].

4. A comienzos de la década de los ochenta se hacía evidente que el procesamiento de datos personales no se limitaba a los ordenadores aislados, sino que se estaba convirtiendo cada vez más en redes. Si bien algunas de estas redes se encontraban enteramente en un país, otras eran de carácter internacional, incidiendo en varias jurisdicciones. El nuevo escenario representó un nuevo desafío para los legisladores nacionales que buscan asegurar una medida de protección de sus ciudadanos. La legislación nacional sobre protección de datos se estaba volviendo obsoleta: ¿cómo se podía garantizar el cumplimiento de una ley nacional cuando sólo una pequeña parte de una red global mucho más grande se encontraba en territorio nacional y cuando las empresas u organizaciones responsables del funcionamiento de la red se encontraban en el extranjero? Esta pregunta, ponía un problema demasiado grande para ser resuelto sólo con las leyes nacionales.

5. En consecuencia, en aquellos años se puso de manifiesto que era necesaria una solución internacional a la cuestión: «*encontrar una base mínima, que sirva de orientación a los Estados sobre esta materia. En este sentido, el desarrollo de reglas internacionales que garanticen, de un modo uniforme, el respeto a la protección de datos y a la privacidad resulta prioritario*»[9]. Los Estados miembros de la UE están sujetos a las normas universales de derechos humanos desarrolladas por la Organización de las Naciones Unidas (en adelante, ONU o Naciones Unidas), que son de aplicación universal[10].

[8] Carlos Eduardo SALTOR (2013: 100).

[9] Sobre la protección de datos personales en el ámbito de la prevención y represión penal, véanse la interesante investigación de Alejandro Luis GACITÚA ESPÓSITO (2014), *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (en busca del equilibrio entre la libertad y la seguridad)*, Tesis Doctoral, Barcelona, Departamento de Ciencia Política y de Derecho Público Universidad Autónoma de Barcelona, mayo, pág. 89.

[10] Como la RESOLUCIÓN DEL CONSEJO DE DERECHOS HUMANOS SOBRE EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL, A/HRC/28/L.27, 24 de marzo de 2015. Disponible en Internet: http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27&referer=/english/&Lang=S [consulta: 10 de julio de 2015]. *Vid*. Monika ZALNIERIUTE (2015), «An international constitutional moment for data privacy in the times of mass-surveillance», en *International Journal of Law and Information Technology*, 0, págs. 1-35. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732448 [consulta: 31 de octubre de 2016].

6. En este sentido, la ONU también se ocupó de la protección de los datos personales. La Resolución 45/95, de 14 de diciembre de 1990, de la Asamblea General de las Naciones Unidas, por la que se aprobaron una serie de principios rectores para la reglamentación de los ficheros computadorizados de datos personales, así como para el establecimiento de unos parámetros globales interestatales en la defensa de la privacidad informática[11]. En concreto, «*establece principios sobre garantías mínimas, y orientaciones sobre archivos de datos personales mantenidos por organizaciones internacionales gubernamentales. Se refiere también a archivos de naturaleza privada*»[12]. No sólo son principios orientadores y recomendaciones que Naciones Unidas realiza a los Estados. Al tiempo, varios órganos y organismos especializados establecidos por los tratados de la ONU se han pronunciado sobre casos concretos, como por ejemplo, en la condena de las prácticas de vigilancia masiva tras las revelaciones de Snowden, entre otros.

7. Antes de centrarnos en la protección europea, cabe mencionar la iniciativa de privacidad de las Directrices de la Organización para la Cooperación y el Desarrollo Económico, el 23 de septiembre de 1980, en la forma de "Recomendaciones", en las cuales, «*no sólo se introducen recomendaciones a los Estados con respecto a la protección de datos personales en el flujo internacional, sino que se delimitan unas líneas básicas de orientación, con respecto a la protección de datos personales en el ámbito nacional o interno*»[13]. Este importante instrumento internacional «*tiene en su texto una relación directa con la protección de los datos de carácter personal, ya que la forma en que esas injerencias se producen en la actualidad es a través del tratamiento automatizado de datos*»[14].

8. La adopción de instrumentos elaborados por organizaciones internacionales como la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) o bien la misma ONU, contribuye a la creación de un marco internacional que permita «*impulsar el respeto a la privacidad y la protección de datos, lo cual supone un positivo avance de*

[11] Teresa GARCÍA-BERRIO HERNÁNDEZ (2003), *Informática y libertades. La protección de datos personales y su regulación en Francia y España*, Murcia, Universidad de Murcia, Servicio de Publicaciones, pág. 61.
[12] Carlos Eduardo SALTOR (2013: 103).
[13] Carlos Eduardo SALTOR (2013: 101); Ana Isabel HERRÁN ORTIZ (1998), *La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson, pág. 58.
[14] Carlos Eduardo SALTOR (2013: 101).

cara a lograr un estándar mínimo de principios, derechos y obligaciones de carácter universal que rijan la materia»[15].

9. También, analizaremos la protección que recibe el derecho a la privacidad en el ámbito del Consejo de Europa para otorgar protección a los ciudadanos que han sufrido vulneraciones dentro de este marco legal mencionando las sentencias más destacadas resueltas por el Tribunal Europeo de Derechos Humanos. En el ámbito específico de la protección de datos personales, el trabajo desarrollado por el Consejo de Europa puede ser calificado de fundador.

10. En primer lugar, el derecho a la privacidad se regula en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950. La definición propuesta en este artículo nos sirve de base para analizar dos cuestiones principales: en el apartado primero, se garantiza la protección a la privacidad y en el apartado segundo, nos encontramos con las limitaciones a este derecho al garantizar la seguridad nacional y la seguridad pública, necesarias para cualquier sociedad democrática. Dicho Convenio creó el Tribunal Europeo de Derechos Humanos para supervisar su cumplimiento a través de la jurisprudencia de dicho Tribunal. En este sentido, nos centraremos en las más importantes decisiones del Tribunal Europeo de Derechos Humanos que permiten apreciar los principios comunes del espacio jurídico europeo sobre la relación entre las medidas de seguridad proporcionadas por los Estados y la protección de la privacidad hasta nuestros días. En el Tribunal Europeo de Derechos Humanos se encuentran de hecho diques sólidos a la proliferación de restricciones al gozo de las libertades debidas a un fortalecimiento de las políticas de seguridad.

11. En los años sesenta, la «*preocupación de las organizaciones supranacionales europeas en la protección de los derechos de la personalidad y en función de las lesiones que los efectos de la tecnología pueden producir en la sociedad*»[16], se determinó en el "Convenio para la protección de las persones con respecto al tratamiento automatizado de datos de carácter personal" (Convenio n. 108) del Consejo de Europa, aprobado en 1981. El Consejo de Europa se considera «*el promotor de la tendencia legislativa en materia de*

[15] Alejandro Luis GACITÚA ESPÓSITO (2014: 89); Alfonso ORTEGA GIMÉNEZ (2015), «La desprotección "internacional" del titular del derecho a la protección de datos de carácter personal», en BARATARIA. Revista Castellano-Manchega de Ciencias Sociales, n. 19, pág. 41.
[16] Carlos Eduardo SALTOR (2013: 102).

protección de datos, superadora de los criterios que existían hasta ese momento, los cuales fueron luego adoptados por muchas leyes y por algunas constituciones europeas»[17].

12. El Convenio n. 108 fue precursor en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales. Efectivamente, «*su contenido no es derecho directamente aplicable, ya que está compuesto por pautas a las que deben acomodarse las legislaciones internas de países que lo han ratificado. Su texto establece una serie de principios básicos para la protección de datos, señala criterios que regulan su flujo y crea un Comité Consultivo, a quien se encomienda la formulación de propuestas para mejorar la aplicación del Convenio*»[18]. Este Tratado internacional es un "Convenio de mínimos", «*ya que se trata de nociones básicas pero fundamentales*». Requiere que los datos sean «*obtenidos y procesados lícitamente, que se registren sobre la base de finalidades legítimas y que no sean utilizados de modo incompatible con esos fines. Promueve que los datos tratados sean exactos, puestos al día, adecuados, pertinentes y no excesivos. Recoge disposiciones acerca de los datos sensibles, medidas de seguridad y mecanismos de cooperación internacional. Exige a las leyes nacionales que lo desarrollen, que lo apliquen en razón del territorio, independientemente de la nacionalidad de los afectados (principio de territorialidad), con el objeto de proteger a los extranjeros en igual alcance que a los nacionales de cada país*»[19].

13. También en el ámbito específico del tratamiento de datos personales por parte de la policía, el Consejo de Europa ha hecho su relevante aporte, al proponer a los Estados miembros la primera Recomendación que orienta la labor policial en el tratamiento de datos personales. Como analizaremos, dicha Recomendación R (87) 15 del Comité de Ministros, para regular la utilización de datos de carácter personal en el sector de la policía, "ha sido referenciada «*por todos los instrumentos normativos elaborados por la Unión Europa referido al tema específico del tratamiento de datos con fines de represión y prevención penal*»[20].

14. Los citados son sólo algunos de los instrumentos dictados por organismos internacionales e instituciones comunitarias que «*reconocen el derecho a la protección de los datos personales como un derecho humano de tercera generación relacionado con los*

[17] Carlos Eduardo SALTOR (2013: 102).
[18] Carlos Eduardo SALTOR (2013: 102).
[19] Carlos Eduardo SALTOR (2013: 103).
[20] Alejandro Luis GACITÚA ESPÓSITO (2014: 127).

derechos a la intimidad»[21], a la "autodeterminación informativa"[22] y «*al desarrollo integral de la personalidad que existe en cada persona con fundamento en su naturaleza humana*»[23]. El fundamento de "ratificar" que el derecho a la protección de los datos de carácter personal es un derecho humano, tal como lo reconoce el derecho internacional, «*radica en las implicaciones jurídicas que esta calificación tiene para todas las personas, en cualquier lugar del planeta. Al incluir a la protección de los datos de carácter personal en el catálogo de derechos humanos, excluimos toda posibilidad de que el derecho interno de cualquier Estado que respete los derechos humanos pueda restringir o desconocer este derecho a quien reclame su aplicación, sea ciudadano o extranjero*»[24].

15. En este sentido, los siguientes apartados tienen por objeto identificar algunas de las iniciativas normativas provenientes de aquellas instituciones internacionales que se han ocupado de la protección de datos personales de los particulares, y que más interesa a nuestra investigación, con el fin de determinar si les ofrecen una tutela adecuada, equilibrada y efectiva en caso de tratamiento ilícito de sus datos personales por los Estados. Esta tutela ha sido también facilitada por el Tribunal Europeo de Derechos Humanos que ha frenado los intentos de fortalecimiento de las herramientas de seguridad que podrían haber dado lugar a una restricción excesiva del derecho a la privacidad. Sobre la cuestión de la privacidad, por tanto, los tribunales supranacionales □nos referimos al Tribunal de Justicia de la Unión Europea, más adelante□ han recurrido recientemente casi al unísono, en defensa de un derecho fundamental potencialmente en riesgo como aquel en objeto.

16. En particular, a continuación, nos vamos a detener en instrumentos internacionales de las siguientes instituciones[25]: 1) la ONU; 2) la OCDE; y 3) el Consejo de Europa.

[21] Carlos Eduardo SALTOR (2013: 106).
[22] Sobre la autodeterminación informativa, *vid*. Adriana MARECOS GAMARRA (2013), «El derecho a la autodeterminación informativa en España y Europa», en *Observatorio Iberoamericano de Protección de Datos*, 25 marzo. Disponible en Internet: https://oiprodat.wordpress.com/2013/03/25/el-derecho-a-la-autodeterminacion-informativa-en-espana-y-europa/ [Consulta: 10 de julio 2015]
[23] Carlos Eduardo SALTOR (2013: 107).
[24] Carlos Eduardo SALTOR (2013: 107).
[25] Estos aportes provienen de distintos centros de producción normativa, tanto de superestructura jurídica internacional (ONU y OCDE), como de los sistemas de integración regional (UE y Consejo de Europa). A pesar de que las distintas organizaciones internacionales están englobadas bajo estructuras de carácter regional, los niveles de integración son muy distintos. *Vid*. Alfonso ORTEGA GIMÉNEZ (2015: 40 y ss.).

2. Protección del derecho de privacidad y de protección de datos personales bajo la regulación de Naciones Unidas

17. Si bien es importante el desarrollo tecnológico para el bienestar de los países, éste no debe ser lesivo de los derechos de sus habitantes; es decir, cualquier estrategia de desarrollo que implique uso y comunicación de información personal está obligada a respetar el derecho a la protección de la información personal, ya que con este derecho se protege a las personas titulares de dicha información.

18. En las siguientes páginas, se verá cómo se ha protegido internacionalmente el derecho a la privacidad, y cómo ha sido su desarrollo para arrojar el nuevo derecho fundamental a la protección de datos personales. El marco de las Naciones Unidas no reconoce la protección de datos personales como un derecho fundamental, aunque el derecho a la privacidad es un derecho fundamental establecido en el orden jurídico internacional. Dentro de la referencia que se hace de cada uno de los instrumentos, se puntualizan las disposiciones que son de interés para nuestro tema, haciendo referencia a distintos aportes que en materia de protección de datos personales deben ser tomados en cuenta por todos los Estados miembros de la sociedad internacional.

2.1. Derecho a la protección de los datos personales como derecho humano autónomo: la Declaración Universal de los Derechos Humanos de 1948. Los avances del Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966

19. Antes de la llegada de nuevas tecnologías que dio lugar a una nueva "declaración de conciencia" sobre el uso de los datos personales, las primeras disposiciones que incidían en el derecho de privacidad y de protección de datos personales, se encontraban dentro de los instrumentos de derecho internacional; citamos, ante todo, la Declaración Universal de los Derechos Humanos de 1948 y el Pacto Internacional de los Derechos Civiles y Políticos de 1966. Estos instrumentos son precursores de todas las legislaciones, nacionales e internacionales, que se ocupan de la materia objeto de nuestra investigación.

20. La preocupación por la protección de los derechos de privacidad expresa la voluntad general, en el día siguiente de la Segunda Guerra Mundial, de borrar los crímenes y ultrajes contra la dignidad humana, estableciendo un sistema completo de reglas para garantizar futuros abusos. Esta misma voluntad se detecta en las disposiciones de la

Declaración Universal de los Derechos Humanos de 1948[26] (en adelante, DUDH), como primer instrumento normativo que consagra los derechos de la persona, para protegerla de arbitrariedades y violaciones que históricamente el individuo había venido padeciendo.

21. En su artículo 3 se consagró que todo individuo tiene «*derecho a la vida, a la libertad y a la seguridad de su persona*»; seguridad que se habrá de entender en su sentido más amplio, considerando así que las injerencias a la vida privada de una persona pueden causar un gravamen a la seguridad física y mental de un individuo. Además, la DUDH establece en su artículo 12 que «*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*»[27]. Con esta disposición el derecho a la privacidad se convierte en parte del catálogo de los derechos humanos fundamentales.

22. La forma en la que se escribió este último artículo aparece tan amplia como para incluir todas las intromisiones directas a una sola persona o un grupo de individuos. En el sentido de las palabras del artículo 12, la expresión "vida privada" se convirtió en un término general para la privacidad, familia, hogar, correspondencia, el honor y la reputación de las personas[28], resultando evidente, ya que las intrusiones en la vida privada de las personas se

[26] La Declaración Universal de Derechos Humanos es considerada generalmente el fundamento de las normas internacionales sobre derechos humanos. La DUDH ha inspirado un valioso conjunto de tratados internacionales de derechos humanos legalmente vinculantes y la promoción de estos derechos en todo el mundo. La Declaración supone el primer reconocimiento universal de que los derechos básicos y las libertades fundamentales son inherentes a todos los seres humanos, inalienables y aplicables en igual medida a todas las personas, y que todos y cada uno de nosotros hemos nacido libres y con igualdad de dignidad y de derechos. DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, adoptada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948. Disponible en Internet: http://www.un.org/es/documents/udhr/law.shtml [consulta: 15 de julio de 2015]. Enric R. BARLETT, María Dolores BARDAJÍ (coords.) (2012), *La Declaración Universal de los Derechos Humanos cumple 60 años. Seminario Permanente de Derechos Humanos Antonio Marzal. XV Sesión*, J.M. Bosch Editor, págs. 168.

[27] Los artículos 3 y 12 se relacionan directamente con el artículo 8 de la DUDH: «*Toda persona tiene derecho a un recurso efectivo ante los tribunales nacionales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la constitución o por la ley*». Este dispositivo pone de manifiesto el derecho de toda persona a contar con un instrumento de protección brindado por el Estado para garantizar sus derechos. Jaime ORAA, Felipe GÓMEZ ISA (1997), *La Declaración Universal de los Derechos Humanos. Un breve comentario en su 50 Aniversario*, Bilbao, Universidad de Deusto, págs. 90. Disponible en Internet: http://www.deusto-publicaciones.es/deusto/pdfs/forum/forum06.pdf [consulta: 15 de julio de 2015].

[28] El derecho a la privacidad representa una anomalía en la historia de los derechos humanos, señalando que, en general, se encuentran con el reconocimiento internacional después de ser consolidados a nivel nacional. En cambio, cuando en la posguerra se construyeron los fundamentos del sistema de derechos humanos, las constituciones nacionales sólo tutelaron aspectos parciales de privacidad, como la inviolabilidad del domicilio y el secreto de la correspondencia. De manera bastante inusual, una garantía general habría sido preparada solamente con los documentos internacionales y, por consiguiente, los sistemas legales nacionales habrían introyectado el enfoque global de la protección de este derecho fundamental, promovido a nivel internacional. *Cfr*. Oliver DIGGELMANN and Maria Nicole CLEIS (2014), «How the Right to Privacy Became a Human Right», en *Human Rights Law Review*, vol. 14, págs. 441-458.

pueden realizar a través de los modernos mecanismos de tratamiento automático de la información. El mismo artículo es de relevante importancia por la tendencia en el reconocimiento del derecho a la protección de los datos personales como derecho humano autónomo, ya que se establece, si bien no de forma específica, este derecho a la protección de información personal, considerando este artículo la base de la protección de datos personales al hablar de injerencias en la vida privada de las personas. Con la DUDH, el derecho a la privacidad se convierte en parte del catálogo[29] de los derechos humanos fundamentales.

23. Sin duda, podemos decir, desde estos primeros artículos, que fue en la ONU donde por primera vez se estableció en un instrumento jurídico internacional un derecho a la protección de la esfera privada de las personas frente a la intrusión de otros, especialmente del Estado, gracias a la DUDH de 1948.

24. No obstante a ello, en la primera mitad del siglo XX, los datos personales no constituían una preocupación fundamental en la vida cotidiana, como es evidente, al no existir la cantidad de avances tecnológicos con los que hoy se interactúan diariamente, situación que propicia la vulnerabilidad del individuo en su vida privada.

25. Como es conocido, la Declaración Universal carece de naturaleza legal convencional. La misma fue adoptada por las Naciones Unidas a través de la Resolución 217 A (III), sin fuerza vinculante, ya que la Asamblea General de las Naciones Unidas no tiene poderes legislativos[30]. Sin embargo, con el paso del tiempo, la Declaración ha ido transformándose en un instrumento que impone ciertas obligaciones a los miembros de las Naciones Unidas. Muchos de los principios establecidos en la DUDH forman parte del *corpus* de normas internacionales, como demuestra el hecho de que existe un notable consenso en la doctrina y en la práctica de los Estados. Este consentimiento se refleja en los acuerdos posteriores y en los tratados internacionales y regionales que se han presentado más adelante, y en las

[29] Entre los artículos que nos interesan, también mencionamos el artículo 29, apartado 2, de la Declaración misma: «*En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática*».

[30] El acto típico que puede emanar según la Carta de las Naciones Unidas es la recomendación, que es una medida de valor meramente exhortativo, destinado a asumir en todo caso una importancia considerable, ya que ha constituido la base para el desarrollo de las normas de carácter consuetudinario. Sin embargo, su contenido se ha traducido en forma jurídicamente vinculante en los dos Pactos de la ONU adoptados en 1966 (*vid*. *infra* en el texto y en las notas).

sentencias de diversos tribunales internacionales así como, más recientemente, en las constituciones y en la legislación interna de cada Estado. Además, la Declaración ha inspirado de manera directa muy diversos acuerdos sobre los derechos humanos, entre ellos el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950[31] (artículo 8) y el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17). En ambos casos, la inspiración del artículo 12 de la Declaración Universal es clara, aunque el Convenio, como veremos más adelante, se aparta de ella en parte, por la inclusión de una serie de excepciones a los derechos protegidos.

26. Siguiendo la línea trazada, en el ámbito de las normas internacionales de derechos humanos, otra referencia a la tutela del derecho a la vida privada está prevista por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas[32] (en adelante, PIDCP), firmado en Nueva York en 1966 y que entró en vigor el 23 de marzo de 1976. El mismo artículo 17 reproduce y desarrolla los principios enunciados en la DUDH previstos en el artículo 12 de la DUDH, aportando elementos importantes a tal respecto: «*1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*». Como se indica, el texto del artículo 17 del Pacto prevé la utilización del adjetivo "ilegales" para calificar la interferencia en la vida privada, en la vida familiar, así como aquellos en el domicilio o su correspondencia, o para definir los delitos y ataques contra el honor y la reputación, la cual está prohibida por la norma[33].

27. También el Pacto reconoce el derecho de todo individuo «*a la libertad y a la seguridad personales*» (artículo 9, apartado 1, Parte III), o al introducir asimismo el derecho de toda persona a la libre circulación señalando que las restricciones sólo son legítimas cuando «*éstas se hallen previstas en la ley, sean necesarias para proteger la seguridad*

[31] *Vid*. *infra*.
[32] En PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en Internet: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx [consulta: 15 de julio de 2015]. Este Acuerdo y el Pacto Internacional de Derechos Económicos, Sociales y Culturales son los primeros instrumentos internacionales jurídicamente vinculantes en materia de derechos humanos, y, junto con la Declaración Universal de los Derechos Humanos de 1948, constituyen el núcleo de la llamada Carta Internacional de Derechos Humanos. La CARTA INTERNACIONAL DE DERECHOS HUMANOS. Disponible en internet: http://www.un.org/es/rights/overview/charter-hr.shtml.
[33] En este sentido, *vid*. Matteo E. BONFANTI (2011), «Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti», en *Diritti umani e diritto internazionale*, vol. 5, núm. 3, págs. 437-481; Oliver DIGGELMANN and Maria Nicole CLEIS (2014).

nacional, el orden público, la salud o la moral públicas o los derechos y libertades de terceros, y sean compatibles con los demás derechos reconocidos en el presente Pacto» (artículo 12, apartado 3, Parte III).

28. Siempre en el ámbito de los instrumentos de tutela de los derechos humanos[34], hay que señalar que el derecho a la vida privada encuentra sitio tanto en la Convención Americana sobre Derechos Humanos de 1969 (Pacto de San José) (artículo 11)[35], como en la Carta Africana sobre los Derechos y el Bienestar del Niño de 1990 (artículo 10)[36].

2.2. Principios básicos de protección de datos en las Directrices para la regulación de los archivos de datos personales informatizados de 1990

29. Ahora bien, en ninguno de todos los instrumentos internacionales en materia de derechos humanos hasta el momento mencionados se hace referencia al concepto del derecho a la protección de los datos personales en sentido estricto. En este sentido, únicamente haciendo una interpretación del texto de los instrumentos internacionales podría vincularse a los datos personales y al tratamiento de estos. Evidentemente, para la época en la que se redactaron estos instrumentos, los avances tecnológicos no representaban el riesgo del manejo de información personal como sucede hoy en día[37]. Pero debido al continuo progreso de la técnica y la informática, consciente de la importancia del tráfico de datos de carácter personal y de las consecuencias que ello puede suponer para el desarrollo de la economía de los estados, ha sido necesario dotar de una cierta autonomía al derecho a la protección de datos personales. Y es que, aunque los instrumentos tradicionales le han

[34] En el 19 de diciembre de 1968 la ONU adopta la Resolución 2450, en la que establece la necesidad de fijar límites a las aplicaciones de la electrónica, por su injerencia en los derechos de la persona, y solicita al Secretario General que prepare un informe donde consten resumidamente los estudios realizados, o en curso, sobre la incidencia de las nuevas tecnologías en los derechos humanos. Se inicia así un período de intensos trabajos sobre la problemática que plantea el alcance de los progresos científicos y tecnológicos en los derechos de la persona, que concluye en 1983, con la aprobación por la Comisión de Derechos Humanos, de un informe relativo al estudio de los principios rectores pertinentes sobre la utilización de los archivos informatizados de datos de carácter personal. *Cfr*. Ana Isabel HERRÁN ORTIZ (1998: 55 y ss.).

[35] Artículo 11 de la CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS de 1969 (Pacto de San José): «*Protección de la Honra y de la Dignidad: 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*».

[36] Artículo 10 de la CARTA AFRICANA SOBRE LOS DERECHOS Y EL BIENESTAR DEL NIÑO de 1990: «*Protección de la intimidad: Ningún niño será objeto de injerencias arbitrarias o ilegales en su intimidad, su familia, su hogar o su correspondencia, ni de ataques a su honor y a su reputación, entendiendo que sus padres o tutores legales tendrán derecho a ejercer una supervisión razonable de la conducta de sus hijos. El niño tiene derecho a la protección de la ley contra tales injerencia o ataques*».

[37] Jonathan LÓPEZ-TORRES (2014), «Antecedentes internacionales en materia de privacidad y protección de datos personales», en *Ejil - EAFIT Journal of International Law*, [S.l.], v. 5, n. 2, págs. 103-117.

dispensado una cierta protección bajo el amparo del derecho a la intimidad, la naturaleza y especificidad de los derechos perjudicados demandan una mejor y mayor cobertura[38].

30. En este orden de ideas, es en 1988 cuando el Comité de los Derechos Humanos de las Naciones Unidas a través de su Observación General número 16 se pronuncia respecto del contenido del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[39], cuyo artículo es la reproducción casi exacta del artículo 12 de la DUDH. En ambos artículos se hace referencia al concepto "vida privada". Sin embargo en la Observación General número 16 en comento se hace referencia al "derecho a la intimidad". En este pronunciamiento, se realiza todo un análisis respecto de qué debe entenderse por injerencias ilegales y arbitrarias a la vida privada, qué se entiende por familia y domicilio. No obstante, en ningún apartado define lo que debe entenderse por vida privada o derecho a la intimidad. Esta disposición impone obligaciones específicas relativas a la protección de la intimidad en las comunicaciones, subrayando lo siguiente en el apartado 8 de la Observación General número 16: «*El cumplimiento del artículo 17 exige que la integridad y el carácter confidencial de la correspondencia estén protegidos de jure y de facto. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones*»[40].

31. Asociado a ello, se realiza un pronunciamiento respecto del tema que nos ocupa en su siguiente apartado 10: «*La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y por que nunca se la utilice para fines incompatibles con el Pacto. Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos*

[38] Alfonso ORTEGA GIMÉNEZ (2015: 41).
[39] OBSERVACIONES GENERALES APROBADAS POR EL COMITÉ DE DERECHOS HUMANOS, Observación general núm. 16, Derecho a la intimidad (artículo 17). Disponible en Internet: https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20DerHum%20%5BCCPR%5D.html#GEN16 [consulta: 15 de julio de 2015].
[40] OBSERVACIONES GENERALES APROBADAS POR EL COMITÉ DE DERECHOS HUMANOS, Observación general núm. 16, Derecho a la intimidad (artículo 17).

de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación»[41].

32. Sobre la base de la Observación General arriba referida, el Comité de los Derechos Humanos de las Naciones Unidas señala, en términos generales, que debe estar regulada la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto para el sector público como el privado, debiéndose adoptar medidas para que la información relativa a la vida privada de una persona no esté disponible para personas no autorizadas para ello. Asimismo, se establece un "derecho de verificación" que consiste en que toda persona tiene el derecho a verificar si hay datos personales suyos almacenados en posesión del sector público o privado, así como un "derecho a saber" cuáles son esos datos almacenados (en caso de haberlos), y para qué fines se han almacenado, así como un "derecho de rectificación o eliminación" en caso de que los datos personales sean incorrectos o si se obtuvieron de forma ilegal, respectivamente[42].

33. Lo planteado, es de suma importancia en virtud de que se establecen los derechos básicos que tiene toda persona respecto del tratamiento de su información personal; aspecto que se conoce en diversas regulaciones y en la literatura en materia de protección de datos personales como "el derecho a la autodeterminación informativa", el cual consiste en el derecho que tiene toda persona para decidir qué se puede hacer o no con su información personal[43].

34. En tal sentido, con la Resolución 45/95, de 14 de diciembre de 1990, la Asamblea General de Naciones Unidas adoptó las "Directrices para la regulación de los archivos de datos personales informatizados"[44]. Se refiere a ciertas garantías mínimas que deberían

[41] OBSERVACIONES GENERALES APROBADAS POR EL COMITÉ DE DERECHOS HUMANOS, Observación general núm. 16, Derecho a la intimidad (artículo 17).
[42] Jonathan LÓPEZ-TORRES (2014).
[43] Jonathan LÓPEZ-TORRES (2014).
[44] En lo que respecta a Naciones Unidas entre 1990 y 1991 se llevó a cabo el 45° periodo de sesiones de su Asamblea General, donde se aprobaron 269 resoluciones, entre las cuales, destaca la Resolución 45/95 de 14 de diciembre de 1990, por la que se aprueban los "Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales". DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, adoptadas mediante resolución 45/95 de la Asamblea

preverse en la legislación nacional con respecto a datos personales y protección de los afectados[45]. La Asamblea solicita a los gobiernos, que tengan en cuenta dichos principios rectores en sus leyes y reglamentos, y que tanto las organizaciones gubernamentales, intergubernamentales como no gubernamentales observen dichos principios en el ámbito de su competencia, lo cual pasa a constituir así uno de los primeros antecedentes en materia de regulación de protección de datos personales.

35. La Resolución es relativamente breve, y está dividida en dos partes: la orientación (A), contiene los principios relativos a las garantías mínimas que deben prever las legislaciones nacionales; y en la orientación (B), la aplicación de las Directrices a archivos de datos personales mantenidos por Organizaciones Internacionales Gubernamentales (OIG).

36. En virtud de los principios rectores básicos en materia de protección de la información personal aprobados por la Asamblea General, los procedimientos para aplicar «*las normas relativas a los archivos de datos personales informatizados se dejan a iniciativa de cada Estado*»[46], con sujeción a una serie de orientaciones, entre las que cabe destacar la relativa a 10 principios que deberían observarse en las legislaciones nacionales[47]: 1) de la legalidad y lealtad; 2) de la exactitud; 3 de finalidad; 4) de acceso de la persona interesada; 5) de no discriminación; 6) facultad de establecer excepciones; 7) de seguridad; 8) control y sanciones; 9) flujo de datos a través de las fronteras; y 10) campo de aplicación.

37. Es importante destacar que este instrumento abre la posibilidad de aplicación también a los documentos no automatizados, así como a los ficheros de personas jurídicas que contengan datos de personas físicas.

General, de 14 de diciembre de 1990. Disponible en Internet: http://www.un.org/es/documents/ag/res/45/list45.htm [consulta: 19 de julio de 2015].

[45] Se aprobaron una serie de principios rectores para la reglamentación de los ficheros computadorizados de datos personales, así como para el establecimiento de unos parámetros globales interestatales en la defensa de la privacidad informática. Teresa GARCÍA-BERRIO HERNÁNDEZ (2003: 61).

[46] DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

[47] Aun cuando se utiliza el término "principio" no todos los señalados lo son en sentido estricto respecto del tratamiento de información personal, pero sí consideramos que son estándares básicos que se deberán observar por las respectivas legislaciones y sujetos regulados, con la finalidad de brindar protección al titular de dicha información. *Vid*. DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990, A. Principios relativos a las garantías mínimas que deben prever las legislaciones nacionales.

38. La orientación B de las Directrices de la ONU de 1990, como mencionado, se refiere a los archivos de datos personales informatizados mantenidos por Organizaciones Internacionales Gubernamentales, «*sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal*», y «*archivos para fines externos, relativos a terceros que tengan relaciones con la organización*»[48]. También se refieren estas Directrices al deber de cada organización de designar a la «*autoridad legalmente competente para supervisar la observancia de estas directrices*»[49], haciendo pues alusión a las Autoridades de control nacional. Por último, en las Directrices se contempla una "cláusula humanitaria" de excepción, que puede preverse específicamente, de aplicación de estos principios en determinados supuestos: «*cuando la finalidad del archivo sea la protección de los Derechos Humanos y las libertades fundamentales de la persona afectada o la ayuda humanitaria*»[50]. También «*debe preverse una excepción similar en la legislación nacional*» a favor de las OIG[51].

39. Por tanto y, como hemos tenido oportunidad de analizar, las Directrices tienen por objeto exhortar la promulgación de leyes sobre privacidad de datos en los Estados miembros de las Naciones Unidas que carezcan de esas legislaciones; y también animar a las organizaciones internacionales a procesar los datos de manera responsable, justa y respetuosa de la privacidad. En cuanto a los flujos de datos transfronterizos, las Directrices de las Naciones Unidas adoptan el principio de reciprocidad.

[48] *Vid*. DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

[49] *Vid*. DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, B. Aplicación de las Directrices a archivos de datos personales mantenidos por Organizaciones Internacionales Gubernamentales.

[50] «*Cláusula humanitaria: puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley*». En DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS.

[51] DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS.

40. Las Directrices aun siendo breves recogen «*los principios básicos de protección de datos, así como la aplicación de éstas, que las organizaciones internacionales deberán tener en cuenta a la hora de llevar a cabo tratamientos de datos de carácter personal*»[52].

41. Su adopción subraya que la privacidad de los datos no es simplemente una preocupación de las sociedades occidentales. Además, en algunos aspectos, los principios de las Directrices de las Naciones Unidas van más allá de algunos de los demás instrumentos internacionales. Sin embargo, las Directrices parecen haber tenido poca influencia en otros instrumentos, como por ejemplo en relación con las Directrices de la OCDE (más adelante) y otros instrumentos[53]. Por tanto, «*la regulación de la protección de datos de carácter personal a nivel internacional se limita a la enunciación de principios que, si bien son de obligado cumplimiento para los Estados miembros de las organizaciones referidas, no implican un gran nivel de detalle ni garantizan la necesaria coherencia, más allá de las líneas de actuación que implican los mencionados principios*»[54]. Las directrices de las Naciones Unidas carecen de fuerza vinculante y los procedimientos para su aplicación quedan a cargo de las iniciativas de cada Estado[55].

2.3. El Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de 2013

42. Desde 2001, los ataques terroristas han creado en el mundo occidental una nueva percepción de vulnerabilidad que se cristalizó, especialmente en los Estados Unidos, en una necesidad genuina de aumentar la seguridad nacional a través de la lucha contra el terrorismo internacional que condujo a la adopción de medidas que generaron limitaciones

[52] Emilia ZABALLOS PULIDO (2013), *La protección de datos personales en España: evolución normativa y criterios de aplicación*, Tesis doctoral inédita de la Universidad Complutense de Madrid, Facultad de Derecho, pág. 97.
[53] Lee A. BYGRAVE (2004), «Privacy Protection in the Global context: A comparative Overview», en *Scandinavian Studies in Law*, vol. 47, pág. 335. Disponible en Internet: http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf [consulta: 23 de julio de 2015].
[54] Emilia ZABALLOS PULIDO (2013: 97).
[55] Sobre este asunto, véase Hurst HANNUM (1996), «The Status of the Universal Declaration of Human Rights in National and International Law», en *The Georgia Journal of International and Comparative Law*, vol. 25, págs. 287-397. Disponible en Internet: http://digitalcommons.law.uga.edu/gjicl/vol25/iss1/13 [consulta: 25 de julio de 2015]; Michael BIRNHACK (2008), «The EU Data Protection Directive: An Engine of a Global Regime», en *Computer Law & Security Report*, vol. 24, núm. 6, pág. 7. Disponible en Internet: https://ssrn.com/abstract=1268744 [consulta: 23 de julio de 2015]; Jochen VON BERNSTORFF (2008), «The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law», en *The European Journal of International Law*, vol. 19, núm. 5, pág. 913. Disponible en Internet: http://www.ejil.org/article.php?article=1710&issue=87 [consulta: 25 de julio de 2015]; Anthony D'AMATO (2010), «Human Rights as Part of Customary International Law: A Plea for Change of Paradigms», en *Faculty Working Papers*, paper 88, págs. 47-98. Disponible en Internet: http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/88 [consulta: 28 de julio de 2015]; Monika ZALNIERIUTE (2015).

considerables a muchos derechos y libertades[56]. Después de los atentados, la Resolución 1373 de 2001 del Consejo de Seguridad de las Naciones Unidas solicitó a todos los Estados a una mayor cooperación en el intercambio de información, especialmente «*en relación con las actividades o movimientos de terroristas* (…) *y la utilización de la tecnología de las comunicaciones por grupos terroristas*»[57]. La Resolución instaba a todos los Estados a tomar medidas para prevenir la comisión de actos terroristas[58], permitiendo una serie de intervenciones que, con el tiempo, han obstaculizado el establecimiento de un equilibrio correcto entre las garantías dadas por los derechos constitucionales y la seguridad nacional. De hecho, muchos Estados priorizaron la seguridad sobre los derechos civiles, estableciendo limitaciones evidentes a los derechos fundamentales de los ciudadanos. Destacan en este punto, por ejemplo, entregas extraordinarias, privaciones arbitrarias de libertad y detenciones, torturas, falta de información pública, juicios injustos, restricciones a la libertad de expresión, violación de privacidad, asesinatos selectivos, *etc*.[59].

43. En este sentido, cabe afirmar que la represión de los grupos terroristas por medio de medidas legislativas[60] excesivamente represivas, como reacción a los acontecimientos

[56] Rosario SERRA CRISTÓBAL (2015a), «The Impact of Counter-Terrorism Security Measures on Fundamental Rights», en *Democrazia & Sicurezza*, Università degli Studi "Roma Tre", anno V, núm. 2, pág. 19. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/DemSic/article/view/432 [consulta: 19 de diciembre de 2015].

[57] RESOLUCIÓN 1373, aprobada por el Consejo de Seguridad en su 4385ª sesión, celebrada el 28 de septiembre de 2001, S/RES/1373 (2001), 28 de septiembre de 2001. Disponible en Internet: http://www.un.org/es/sc/ctc/resources/res-sc.html [consulta: 19 de diciembre de 2015].

[58] En su expresión de apoyo y solidaridad, la Unión Europea declaró «*que la lucha contra el terrorismo será más que nunca un objetivo prioritario de la Unión Europea*». *Vid*. CONCLUSIONES Y PLAN DE ACCIÓN DEL CONSEJO EUROPEO EXTRAORDINARIO de 21 de septiembre de 2001, DOC/01/13, Bruselas, le 21 septiembre 2001. Disponible en Internet: http://europa.eu/rapid/press-release_DOC-01-13_es.htm [consulta: 28 de diciembre de 2015]. El Consejo de la Unión Europea solicitó a la Comisión Europea que presentara propuestas para garantizar que las autoridades encargadas de hacer cumplir la ley puedan investigar actos delictivos que impliquen el uso de sistemas de comunicaciones electrónicas y adoptar medidas legales contra los autores de esos actos. SESIÓN EXTRAORDINARIA DEL CONSEJO - JUSTICIA, ASUNTOS DE INTERIOR Y PROTECCIÓN CIVIL, C/01/327, Bruselas, 20 de septiembre de 2001. Disponible en Internet: http://europa.eu/rapid/press-release_PRES-01-327_es.htm [consulta: 19 de diciembre de 2015].

[59] Rosario SERRA CRISTÓBAL (2015a: 20).

[60] En este sentido, se observa como en Francia han sido adoptadas medidas en las que se puede inhibir el acceso a un sitio web mediante el bloqueo de sistema de nombres de dominio (*DNS*, por sus siglas en inglés, *Domain Name System*) de ciertos sitios sin la intervención de un juez, pero sólo con la intervención de una comisión específica en el caso de que el contenido del sitio web haga referencia a pornografía infantil o terrorista. DÉCRET n. 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. Así como se puede mencionar la nueva Ley sobre los servicios de inteligencia adoptada el 24 de junio de 2015 en Francia por la Asamblea Nacional francesa (LOI n. 2015-912 du 24 juillet 2015 relative au renseignement). La ley, permite el uso de herramientas de vigilancia masiva que captan llamadas de teléfonos móviles y de cajas negras (con fines antiterroristas) en los proveedores de servicio de Internet que recogen y analizan los datos personales de millones de usuarios de Internet. Detrás de este control, la ley no plantea una única razón para luchar contra el terrorismo internacional, sino también la protección de la defensa nacional, los de política exterior importantes, la protección de intereses económicos, industriales y científicos de Francia, y prevenir la violencia colectiva y la delincuencia organizada. «Francia: Nueva ley de vigilancia, duro golpe para los

trágicos como los ocurridos en Francia y Bélgica, ha ganado mayor aceptación entre la comunidad internacional después de los atentados terroristas de Nueva York del 11 de septiembre de 2001.

44. En 17 de abril de 2013, la Asamblea General de Naciones Unidas emitió un "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión", presentado al Consejo de Derechos Humanos en su 23º período de sesiones[61], en el que se argumenta que los Estados han utilizado las nuevas tecnologías para fortalecer las medidas de vigilancia contra los ciudadanos, poniendo en peligro el pleno disfrute de los derechos humanos a la privacidad, a la libertad de opinión y expresión.

45. La otra cara de la moneda del uso de las nuevas herramientas tecnológicas en un marco internacional es que algunos Estados operan como un "Gran Hermano", con el derecho a la privacidad seriamente limitado por las necesidades de seguridad nacional invocadas cada vez que hay que tomar una medida que supone un paso atrás en la protección de los derechos humanos. Mientras que, de un lado, la red ha ayudado a fortalecer la libertad de expresión, por otro lado, sin embargo, ha favorecido introducir nuevas modalidades de vigilancia. Es necesario, por lo tanto, imponer a los Estados una reglamentación en función con los derechos humanos. Muchos, de hecho, están desarrollando cada vez más los controles sobre los móviles, la red y correos electrónicos. En el Informe, el Relator Especial, destaca la importancia de las intercepciones como herramienta útil para la lucha contra la criminalidad, incidiendo en que en todo caso deben ser autorizadas por el tribunal. En cambio, algunos países han debilitado los controles y desplazado el poder en manos de los gobiernos[62].

46. En las conclusiones y recomendaciones finales del Informe de abril de 2013[63], el Relator Especial reconoce que la vigilancia de las comunicaciones debe considerarse un «*acto sumamente perturbador que podría suponer una injerencia en los derechos a la*

derechos humanos», en *Amnistía Internacional España*, 24 de julio de 2015. Disponible en Internet: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/francia-nueva-ley-de-vigilancia-duro-golpe-para-los-derechos-humanos/ [consulta: 14 de diciembre de 2015].

[61] Frank LA RUE (2013), «Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión», Naciones Unidas, Asamblea General, A/HRC/23/40, 17 de abril de 2013, págs. 1-24.

[62] "En el Reino Unido, por ejemplo, el Secretario de Estado autoriza la interceptación de las comunicaciones; en Zimbabue, lo hace el Ministro de Transporte y Comunicaciones". Frank LA RUE (2013: 15).

[63] El Relator Especial insta a los Estados a adoptar las normas y reglas que garantizan la seguridad de las comunicaciones a cada individuo y, en particular, periodistas, activistas y denunciantes de derechos humanos. En este sentido, *vid*. Frank LA RUE (2013: 22).

libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática». En la elaboración de medidas de vigilancia de las comunicaciones (y escuchas telefónicas) es necesario que: «*estén en consonancia con la ley, cumplan con las normas de claridad y precisión suficientes para que las personas sean notificadas por adelantado y puedan prever su aplicación; b) sean estricta y fehacientemente necesarias para lograr un objetivo legítimo; y c) se ajusten al principio de proporcionalidad y no se empleen cuando se disponga de técnicas menos invasivas o cuando estas no se hayan agotado*»[64]. También solicita a los Estados castigar severamente la vigilancia ilegal por los agentes públicos o privados.

2.4. La Resolución sobre "El derecho a la privacidad en la era digital" de 2013

47. Sólo unos meses después del Informe del Relator Especial de 17 de abril de 2013, sale a la luz el caso de las escuchas telefónicas y espionaje realizadas por la *National Security Agency* (*NSA*) de Estados Unidos y los servicios secretos de Reino Unido, Australia, Nueva Zelanda y Canadá, que afecta de forma directa incluso a algunos presidentes de los gobiernos europeos, entre ellos los de Alemania e Italia.

48. Después de estos acontecimientos, algunos gobiernos han reaccionado con prontitud llevando el asunto a Naciones Unidas[65]. En este punto, se aspira a regular la adquisición ilegal de datos a través de la red, dimensionada en términos de protección de la privacidad como derecho humano, como muestra la Resolución aprobada por la Asamblea General de las Naciones Unidas 68/167[66], aprobada por unanimidad el 18 de diciembre de 2013, sobre

[64] Frank LA RUE (2013: 23).

[65] A pesar de la aparente sorpresa e indignación de algunos jefes de Estado europeos, se supo más tarde, con el lanzamiento de nuevos documentos por el mismo Snowden, que algunos países europeos, como Francia, Alemania, España, Suecia y el Reino Unido, habían actuado en concierto con la *NSA* en las prácticas de la vigilancia global y que habían compartido con los Estados Unidos enormes cantidades de datos. En este sentido, el director de inteligencia nacional de Estados Unidos, James Clapper, declaró, de hecho, en el Congreso de Estados Unidos que el asombro de los gobiernos europeos fue al menos en parte hipócrita, ya que la vigilancia se había llevado a cabo con el apoyo de las agencias de inteligencia locales: «*Some of this reminds me of the classic movie Casablanca: "My God, there's gambling going on here"*». *Cfr*. Julian BORGER (2013), «GCHQ and European spy agencies worked together on mass surveillance», en *The Guardian*, Fri 1 Nov 2013. Disponible en Internet: https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden [consulta: 25 de octubre de 2016].

[66] RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2013, 68/167, El derecho a la privacidad en la era digital, A/RES/68/167, 21 de enero de 2014. Disponible en Internet: http://www.un.org/es/comun/docs/?symbol=A/RES/68/167 [consulta: 29 de octubre de 2016]. En diciembre de 2013, por iniciativa de Brasil y Alemania, junto con Austria, Liechtenstein, México, Noruega y Suiza, la Asamblea General de las Naciones Unidas adoptó la Resolución 68/167, en la que se expresaron profundas preocupaciones por el impacto negativo de los programas de vigilancia y espionaje en el disfrute de los derechos humanos.

"El derecho a la privacidad en la era digital"[67]. En esta Resolución la Asamblea General está «*profundamente preocupada*» por los «*efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala*», y recuerda a los Estados revisar los procedimientos y normas sobre la interceptación, recopilación y conservación de datos, con el fin de reforzar la protección de los derechos humanos. También se les invita a establecer mecanismos específicos para una mayor transparencia y responsabilidad de los Estados en el ámbito de la vigilancia de las comunicaciones[68]. El carácter extraterritorial de este tipo de vigilancia fue señalado como un aspecto particularmente preocupante de la cuestión porque los Estados se consideran garantes de hacer cumplir los derechos humanos en su territorio. Así que la Resolución los instaba a respetar la privacidad y revisar sus procedimientos, prácticas y legislaciones, de un modo que permita establecer mecanismos independientes y efectivos para asegurar la transparencia y la responsabilidad de cada Estado.

49. La Resolución 68/167 está inspirada en el hecho de que los avances tecnológicos permiten a los individuos, empresas y gobiernos utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementan la capacidad de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos de forma ilegal, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad[69], en violación del artículo 12 de la DUDH y el artículo 17 del PIDCP[70] (*vid*. *supra*).

50. Obviamente, el derecho a la privacidad, al igual que la mayoría de los derechos humanos, no es absoluto, sino que puede dar lugar a excepciones. Estas excepciones, como se indica en uno de los considerandos de la Resolución 68/167, sin embargo, deben cumplir

[67] Una visión de síntesis, en la página web de Naciones Unidas "*The Right to Privacy in the Digital Age*". Disponible en Internet: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx [consulta: 30 de octubre de 2016].

[68] RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2013, 68/167.

[69] Aunque las resoluciones de la Asamblea General de las Naciones Unidas no son jurídicamente vinculantes (derecho blando o *soft law* en inglés), desencadenaron un importante debate internacional de alto nivel sobre la privacidad, las nuevas tecnologías y la vigilancia, y son consideradas como un importante primer paso para la regulación de la materia.

[70] Ambas disposiciones protegen al individuo de interferencias arbitrarias en su vida privada, familiar, hogar y correspondencia. Las disposiciones en cuestión se adoptaron en la era pre-digital (la Declaración es de 1948, mientras que el Pacto de 1966), pero su contenido se puede adaptar fácilmente a los tiempos modernos. Monika ZALNIERIUTE (2015).

con todas las demás obligaciones que se derivan del respeto de los derechos humanos[71], como por ejemplo el artículo 8 del Convenio Europeo de Derechos Humanos (véase *amplius infra*).

51. Leyendo el texto de la Resolución 68/167, en la parte dispositiva[72], ésta «*exhorta*» a todos los Estados a que «*respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales*»; «*adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos*». Además, prevé que los Estados «*examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos*». Por último, se recomienda que «*establezcan o mantengan mecanismos nacionales de supervisión independientes* (es decir, autoridades de control nacional) *y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado*»[73].

52. Como resultado, la Asamblea General de las Naciones Unidas solicitó a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos (en adelante, ACNUDH) que preparara un informe sobre el derecho a la privacidad en la era digital. En palabras de la Resolución 68/167, el informe consistía en examinar «*la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala*».

[71] Eso también se aplica a la lucha contra el terrorismo internacional. La Resolución reitera, de hecho, que las medidas adoptadas por los Estados para combatir el terrorismo deben respetar el derecho internacional, incluyendo las obligaciones en virtud de los derechos humanos, derecho humanitario y derecho de los refugiados. De importancia es que la Resolución, con referencia a los acontecimientos recientes, expresa profunda preocupación por la interceptación extraterritorial y para la adquisición de datos a gran escala.

[72] RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2013, 68/167, pág. 2.

[73] Paréntesis y no cursivas añadidas por mí. RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2013, 68/167, pág. 3.

53. El Informe de la ACNUDH fue presentado al Consejo de Derechos Humanos en su vigésimo séptimo período de sesión (septiembre de 2014) y a la Asamblea General en su sexagésima novena período de sesión (diciembre de 2014)[74]. El ACNUDH animó a todas las partes interesadas para compartir informaciones y perspectivas sobre las cuestiones planteadas en la Resolución 68/167[75]. El Informe denuncia que la existencia de programas de vigilancia a gran escala constituye una injerencia desproporcionada en el derecho a la privacidad. Se observó que, si bien hubo un interés público en la lucha contra el terrorismo, ésta no puede justificar las medidas de vigilancia sin límite, ya sea con respecto a las categorías de personas implicadas en la medida, ya sea a su duración.

54. El Informe subraya, sin embargo, los nuevos retos de la vigilancia electrónica, para lo cual los Estados nacionales, para acceder a los datos relacionados con las comunicaciones, deben adoptar un marco normativo claro, preciso, accesible, incluyente y no discriminatorio, con el fin de una mayor transparencia, con respecto a las políticas y la legislación de vigilancia y las interpretaciones legales y las resoluciones judiciales, en su caso, que incorporen los avances en la tecnología y estén en conformidad con el Estado de Derecho y las normas internacionales de derechos humanos. Una mejor aplicación a nivel nacional de las normas internacionales relativas al derecho a la privacidad requiere una legislación nacional adecuada y unas garantías y una supervisión más sólidas[76].

55. En particular, cualquier injerencia en el derecho a la privacidad debía cumplir los principios de legalidad, necesidad y proporcionalidad y los Estados deben garantizar una

[74] En su Decisión 25/117, aprobada en marzo de 2014, el Consejo de Derechos Humanos decidió convocar en su 27º período de sesiones una mesa redonda sobre la promoción y protección del derecho a la privacidad en la era digital. Esto se realizó en un contexto de vigilancia nacional y extraterritorial, de interceptación de las comunicaciones digitales y la recopilación de datos personales, incluso a gran escala, con el fin de identificar los desafíos y las mejores prácticas. El Consejo de Derechos Humanos pidió al Alta Comisionada que organizara una mesa redonda con los Estados, los órganos pertinentes de las Naciones Unidas, la sociedad civil, las organizaciones no gubernamentales, el sector privado y las instituciones nacionales de derechos humanos. El debate tuvo lugar el 12 de septiembre de 2014. El ACNUDH preparó entonces un informe resumen sobre los resultados, que se presentó al Consejo de Derechos Humanos en su 28º período de sesiones. *Vid*. RESUMEN DE LA MESA REDONDA DEL CONSEJO DE DERECHOS HUMANOS sobre el derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, A/HRC/28/39, 19 de diciembre de 2014, págs. 1-18. Disponible en Internet: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39&referer=http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx&Lang=S [consulta: 29 de octubre de 2016].

[75] Para facilitar una mejor interpretación a los Estados miembros, véase Nota de 26 de febrero de 2014 adjunta a la Resolución aprobada por la Asamblea General el 18 de Diciembre de 2013. Disponible en Internet: http://www.ohchr.org/Documents/Issues/Privacy/NV.pdf [consulta: 29 de octubre de 2016].

[76] RESUMEN DE LA MESA REDONDA DEL CONSEJO DE DERECHOS HUMANOS sobre el derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, A/HRC/28/39, 19 de diciembre de 2014, págs. 13 y ss.

supervisión eficaz y remedios efectivos contra las violaciones de la privacidad por medio de la vigilancia digital[77].

56. Como es evidente, cualquier excepción permitida por ley al ejercicio de un derecho humano debe darse solamente con un objetivo legítimo y solamente para cumplir dicho objetivo. No debe existir otra alternativa menos intrusiva para alcanzarlo y, por supuesto, debe haber garantía judicial ante cualquier interferencia estatal sobre la vida de los ciudadanos. Con respecto a las interferencias originadas en empresas privadas, el Estado debería ejercer su rol de garante de los derechos humanos y establecer políticas para asegurar una adecuada gestión de los datos personales.

57. ¿Qué ocurre si la vulneración de la privacidad no se orienta hacia un individuo en particular, sino que es masiva e indiscriminada? Claramente, eso constituye una violación masiva de los derechos humanos[78].

---

[77] La Asamblea General aprobó la Resolución 69/166, de 18 de diciembre de 2014, en su sexagésimo noveno período de sesiones, tomando nota con interés del informe del ACNUDH sobre "El derecho a la privacidad en la era digital". RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2014, 69/166, El derecho a la privacidad en la era digital, A/RES/69/166, 10 de febrero de 2015. Disponible en Internet: http://www.un.org/es/comun/docs/?symbol=A/RES/69/166 [consulta: 29 de octubre de 2016]. El 24 de marzo de 2015 se publicó la Resolución de Naciones Unidas titulada "El derecho a la privacidad en la era digital", que establece que el marco legal para la vigilancia debe estar claro y ser públicamente accesible y considera la intercepción de los metadatos de las comunicaciones un acto intrusivo. También solicita al Consejo de Derechos Humanos de las Naciones Unidas la creación de un Relator Especial para el Derecho a la Privacidad. Exhortando a todos los Estados a que respeten y protejan el derecho a la intimidad, la Asamblea General animó al Consejo de Derechos Humanos a considerar la posibilidad de establecer un procedimiento especial para promover este objetivo. *Vid*. RESOLUCIÓN DEL CONSEJO DE DERECHOS HUMANOS SOBRE EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL, A/HRC/28/L.27. En abril del 2015, finalmente, el Consejo de Derechos Humanos aprobó en su 28º período de sesiones la Resolución 28/16, por la que decidió nombrar por un período de tres años un "*Special Rapporteur on the right to privacy*" (Relator Especial sobre el derecho a la privacidad). El Relator Especial es un experto independiente designado por el Consejo de Derechos Humanos para examinar e informar acerca de una situación violación del derecho de la privacidad en un país o sobre un tema específico de derechos humanos, incluso en relación con los desafíos derivados de las nuevas tecnologías. Se pidió a los Estados que cooperaran plenamente y prestaran asistencia al Relator Especial. Los Relatores Especiales son parte de los procedimientos especiales del Consejo de Derechos Humanos. En julio de 2015 fue nombrado como "*Special Rapporteur on the right to privacy*" el Prof. Joseph Cannataci. Con referencia al Relator Especial sobre el derecho a la privacidad, véanse página web de las Naciones Unidas: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx [consulta: 30 de octubre de 2016].

[78] Así se expresó Ben Emmerson, consejero de la reina en Reino Unido y relator especial de la ONU sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo: «*El derecho internacional de los derechos humanos exige que los Estados justifiquen con claridad y pruebas cualquier injerencia en el derecho a la privacidad, ya sea individual o a gran escala. Es axioma central de la proporcionalidad que cuanto mayor sea la injerencia en los derechos humanos protegidos, más convincente deberá ser la justificación* (…). *La dura realidad es que el uso de la tecnología de vigilancia a gran escala realmente suprime por completo el derecho a la privacidad de las comunicaciones en Internet.* (…) *Además, permite interferir en las comunicaciones privadas sin autorización independiente o previa, o de cualquier otro tipo, sobre la base de la sospecha que se tiene de una persona u organización en particular.* (…) *Las comunicaciones de literalmente todos los usuarios de Internet pueden ser inspeccionadas por los organismos de inteligencia y encargados de hacer cumplir la ley en estos Estados. Esta práctica equivale a una injerencia sistemática en el derecho al respeto de la privacidad* (…) *y, en consecuencia, requiere una*

58. Mientras que las resoluciones anteriores se centraron en los efectos negativos de la vigilancia masiva y la responsabilidad de los Estados para restringir los poderes de las autoridades de inteligencia, las resoluciones más recientes reflejan un desarrollo clave en el debate sobre la privacidad en las Naciones Unidas. Las Resoluciones adoptadas en 2016 y 2017 reafirman la necesidad de limitar los poderes de las agencias de inteligencia y condenar la vigilancia masiva[79]. Sin embargo, también afirman explícitamente que la creciente capacidad de las empresas comerciales para recopilar, procesar y utilizar datos personales puede suponer un riesgo para el disfrute del derecho a la privacidad en la era digital. Por lo tanto, además de la responsabilidad de las autoridades estatales, las últimas Resoluciones apuntan a la responsabilidad del sector privado de respetar los derechos humanos, y exigen que las empresas informen a los usuarios sobre la obtención, uso, intercambio y conservación de datos personales y establezcan políticas de procesamiento transparentes.

3. El desafío de la protección de la intimidad y la circulación transfronteriza de datos personales en la OCDE

59. En defensa de la persona, y del libre ejercicio de sus derechos frente al progresivo desarrollo de los medios informáticos de tratamiento de la información, pronto resultan ineficaces los instrumentos jurídicos de defensa que hasta ese momento le son reconocidos con carácter general al individuo. Es decir, que los medios de defensa y prevención de injerencias en la intimidad y vida privada no son suficientes para la protección de la persona frente a las intromisiones procedentes de una utilización abusiva o ilegítima de la informática. En este orden de ideas, también la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha desempeñado un papel importante en materia de protección de la información personal en el contexto internacional[80].

justificación convincente. (…) *La privacidad puede definirse como la presunción de que el individuo debe tener una esfera de desarrollo autónomo personal, interacción y libertad, libre de la intervención del Estado y de la intrusión excesiva* (…). *El deber de respetar la privacidad y la seguridad de las comunicaciones implica que las personas tienen derecho a compartir información e ideas entre sí sin la injerencia del Estado (o de un agente privado), con la certeza de que sus comunicaciones llegarán a sus destinatarios y solo estos las leerán. El derecho a la privacidad también incluye el derecho de las personas a saber quién posee información sobre ellas y cómo se utiliza*». En NOTA DEL SECRETARIO GENERAL, Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/69/397, 23 de septiembre de 2014. Disponible en Internet: http://repository.un.org/bitstream/handle/11176/158700/A_69_397-ES.pdf?sequence=6&isAllowed=y [consulta: 01 de noviembre de 2016].

[79] RESOLUTION ADOPTED BY THE HUMAN RIGHTS COUNCIL ON 23 MARCH 2017, The right to privacy in the digital age, A/HRC/RES/34/7, 7 April 2017.

[80] Alejandro Luis GACITÚA ESPÓSITO (2014: 92 y ss.).

60. Si bien ésta es una organización enfocada al desarrollo económico[81], en el seno de la misma Organización se percibió la problemática derivada de las diversas estrategias de desarrollo en materia de comercio, en particular en lo concerniente al comercio electrónico, pues éste implica el intercambio, manejo, uso y tratamiento en general de la información personal. En este sentido, los países miembros de la OCDE han elaborado leyes para la protección de la intimidad, si bien sus disparidades en la legislación creaban obstáculos a la libre circulación de información entre los países[82].

3.1. Directrices sobre protección de la privacidad y flujos transfronterizos de datos de 1980

61. La adopción de las "Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales" (en inglés, "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*")[83], que fueron aprobadas mediante una

[81] La OCDE nace al igual que otras instituciones (como la ONU o el Consejo de Europa) después de la Segunda Guerra Mundial, con un objetivo claro de mejorar la vida y las relaciones entre los países evitando que una nueva guerra pudiera llegar. La Organización Europea de Cooperación Económica (OECE), origen de la actual OCDE, surge en 1948 para llevar a cabo el Plan Marshall financiado por Estados Unidos para reconstruir Europa. La OCDE, tuvo su origen en la Convención de la OCDE el 14 de diciembre de 1960. La OCDE nació oficialmente el 30 de septiembre de 1961, fecha de entrada en vigor de la Convención. La OCDE «*is an international organisation that works to build better policies for better lives. Our goal is to shape policies that foster prosperity, equality, opportunity and well-being for all. We draw on almost 60 years of experience and insights to better prepare the world of tomorrow. Together with governments, policy makers and citizens, we work on establishing international norms and finding evidence-based solutions to a range of social, economic and environmental challenges. From improving economic performance and creating jobs to fostering strong education and fighting international tax evasion, we provide a unique forum and knowledge hub for data and analysis, exchange of experiences, best-practice sharing, and advice on public policies and global standard-setting*». *Vid*. The Organisation for Economic Co-operation and Development (OECD), accesible en Internet: http://www.oecd.org/about/ [consulta: 01 de noviembre de 2016].

[82] En 1969, la OCDE inició unos estudios sobre la utilización de los ordenadores en el sector público, dando lugar al programa sobre los flujos de datos transfronterizos que más tarde serían la base de las directrices sobre la privacidad. «*Un Grupo de Expertos, el Data Bank Panel, analizó y estudió diferentes aspectos de la cuestión de la intimidad, verbigracia, en relación a la información digital, la administración pública, la circulación transfronteriza de datos y los resultados implícitos de la política en general. A fin de recabar pruebas de la índole de los problemas, el Data Bank Panel organizó un Simposio en Viena en 1977, que proporcionó opiniones y experiencia procedentes de una diversidad de sectores interesados, incluidos gobiernos, industria, usuarios de redes internacionales de comunicación de datos, servicios de tratamiento y organismos intergubernamentales*». En DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980), 23 de septiembre de 1980. «*A principios de 1978 se creó dentro de la OCDE un nuevo Grupo de Expertos ad hoc sobre las Trabas a la Circulación Transfronteriza de Datos y Protección de la Intimidad, al que se encargó la elaboración de directrices sobre normas básicas que rijan la circulación transfronteriza y la protección de datos personales y de la intimidad, a fin de facilitar la armonización de las legislaciones nacionales, sin perjuicio de que se establezca en fecha posterior un Convenio internacional*». Esta labor consistió en la adopción, antes del 1º de julio de 1979, de unas directrices sobre normas básicas reguladoras del flujo internacional de datos y la protección de datos personales. *Vid*. DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980). También, *vid*. María del Carmen GUERRERO PICÓ (2006), *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, Thomson-Civitas, págs. 47 y ss.

[83] Página web en inglés de OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [consulta: 25 de octubre de 2015].

Recomendación del Consejo de la OCDE y que entró en vigor el de 23 septiembre de 1980, se basa en la falta de uniformidad en la regulación de protección de la privacidad y flujos transfronterizos de datos personales en los distintos Estados miembros[84]. De acuerdo con el prólogo de las Directrices, «*existe el peligro de que las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de datos personales* (…)*. Por este motivo, los países miembro de la OCDE han considerado necesario elaborar Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos*. *Representan un consenso sobre principios básicos que pueden incorporarse a la legislación nacional existente o servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella*»[85].

62. Este interés en la protección del derecho a la protección de datos y la percepción del peligro de que «*las disparidades en las legislaciones nacionales pudieran obstaculizar la libre circulación transfronteriza de los datos personales*» con los «*graves trastornos*» que ello «*podría ocasionar en importantes sectores de la economía, como la banca y los seguros*», fueron las principales motivaciones para la elaboración de las Directrices[86]. La importancia de estas se basa en que representan un consenso sobre «*principios básicos*» reguladores del derecho a la privacidad que, adoptados sin disparidades por los Estados, garanticen la ausencia de «*obstáculos a la libre transferencia internacional de datos entre los países*»[87].

63. La relevancia de la Directrices de la OCDE de 1980 reside «*en ser el primer documento de ámbito supranacional que analiza en profundidad el derecho a la protección*

[84] La Recomendación del Consejo de la OCDE, introdujo importantes reformas en sus legislaciones estatales con el fin impedir el almacenamiento ilícito de datos personales y su revelación no autorizada. Esta situación provocó con el tiempo una lógica preocupación por proteger la intimidad de los ciudadanos, lo que dio lugar a un desarrollo asimétrico de normas nacionales y, por consiguiente, un inevitable obstáculo a la libre circulación transfronteriza de datos. *Vid*. Alfonso ORTEGA GIMÉNEZ (2015: 41-42).

[85] En DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980).

[86] Las Directrices fueron elaboradas por un grupo de expertos gubernamentales. Fueron acompañadas de un «*Memorándum Explicativo, con la finalidad de proporcionar información acerca del debate que se llevó a cabo y de los razonamientos que subyacen en su planteamiento*». En el mismo se destaca como, «*entre los países miembros de la OCDE, más de un tercio*» habían promulgado a la fecha una o varias leyes «*para proteger a las personas frente al uso abusivo de los datos que a ellos se refieren y darles el derecho de acceso a los mismos con vistas a comprobar su exactitud e idoneidad*». *Vid*. DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 8).

[87] *Vid*. DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 7).

de datos de carácter personal»[88]. Estas Directrices son también significativas desde la perspectiva de que representan el primer Acuerdo Transatlántico sobre la protección de la privacidad[89].

64. Tales Directrices están presentes en un Anexo a la Recomendación del Consejo que forma parte de ésta, y se estructura en cinco partes diferenciadas. La primera parte de carácter general, que son normas "*minimum*" (apartados de 1 a 6), establece las definiciones aplicables, incluyendo específicamente los conceptos de dato personales, responsables del tratamiento (mejor dicho, según la terminología del texto «*controlador de datos*»), afectado y transferencia internacional de datos. Además, establece determinados principios referidos a su ámbito de aplicación, «*a fin de que no pueda considerarse que el establecimiento de los estándares*»[90] previsto en las Directrices pueda implicar una reducción del respeto a la intimidad. Del mismo modo, se indica que las Directrices son aplicables a los sectores público y privado y «*que las mismas constituyen un catálogo de mínimos en esta materia*»[91].

65. En la segunda parte, las Directrices (apartados de 7 a 14) vinieron a establecer ocho principios básicos de aplicación nacional que han de regir el tratamiento de datos de carácter personal que pudiera ser adoptado en esta materia. Estos principios, constituyen la raíz de las normas nacionales e internacionales adoptadas en materia de protección de datos con posterioridad[92], y pueden resumirse en: "principio de limitación de la recogida"; "principio de calidad de los datos"; "principio de especificación de la finalidad"; "principio de limitación de uso"; "principio de salvaguardas de seguridad"; "principio de apertura"; "principio de participación individual" y "principio de responsabilidad"[93].

[88] Alejandro Luis GACITÚA ESPÓSITO (2014: 92). Estos documentos no son jurídicamente vinculantes, sino más bien meras disposiciones mínimas que recomiendan a los Estados seguir una serie de principios generales en materia de tratamiento de datos personales. *Cfr*. Mónica ARENAS RAMIRO (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, págs. 638.

[89] Avner LEVIN and Mary JO NICHOLSON (2005), «Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground», en *University of Ottawa Law & Technology Journal*, vol. 2, núm. 2, pág. 375. Disponible en internet: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=894079 [consulta: 05 de diciembre de 2015].

[90] Alejandro Luis GACITÚA ESPÓSITO (2014: 98).

[91] Alejandro Luis GACITÚA ESPÓSITO (2014: 98); DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 3-4).

[92] *Vid*. Agustín PUENTE ESCOBAR (2006), «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en Álvaro CANALES GIL, María José BLANCO ANTÓN, José Luis PIÑAR MAÑAS, Mercedes ORTUÑO SIERRA (coords.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Valencia, Tirant lo Blanch, págs. 37-68.

[93] Para un mayor desarrollo de los mismos: «*Principio de limitación de la recogida. 7. Debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos. Principio de calidad de los datos. 8. Los*

66. La tercera parte (apartados de 15 a 18) se centra en los principios básicos de aplicación internacional, con enfoque a la libre circulación transfronteriza de datos de carácter personal y restricciones legítima, de forma que se garantice el libre flujo de estos. En este sentido, el apartado 16 exige a los Estados miembros garantizar la seguridad del tráfico de la información[94]. El requisito para que proceda la transferencia internacional de datos es que el Estado de destino «*haya observado sustancialmente estas Directrices*». Además, podrán establecerse restricciones adicionales en relación con «*ciertas categorías de datos personales para las cuales su legislación nacional sobre la intimidad incluya normativas específicas en vista de la índole de tales datos y para las cuales otro país miembro no proporcione protección equivalente*»[95].

67. La importancia de estos «*principios básicos comunes divididos en principios de aplicación nacional e internacional* (…) *se demuestra en el hecho de que el documento número 12 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, considera que el cumplimiento de éstos por parte de los Estados viene a constituir el mínimo necesario para*

datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día. Principio de especificación de la finalidad. 9. Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad. Principio de limitación de uso. 10. Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo: a) con el consentimiento del sujeto de los datos, o b) por imperativo legal. Principio de salvaguardas de seguridad 11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados. Principio de apertura 12. Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos. Principio de participación individual 13. La persona debería tener derecho a: a) recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma; b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible; c) que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, y d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos. Principio de responsabilidad 14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba». En DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 4-5).

[94] DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 5), apartado 16: «*Los países miembro deberían adoptar todas las medidas razonables y oportunas para garantizar la circulación transfronteriza, ininterrumpida y segura, de los datos personales, incluso el tránsito a través de algún país miembro*».

[95] DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 5-6), apartado 17.

que los mismos puedan ser considerados como oferentes de un nivel adecuado de protección de datos»[96].

68. Por último, la cuarta y quinta parte de las Directrices de 1980 (apartado de 19 a 22) regulan respectivamente las medidas de «*implantación nacional*» de las Directrices y la «*cooperación internacional*» entre los Estados miembros[97]. En cuanto a las medidas de implantación nacional, se indica en el apartado 19 el deber de los Estados miembros de «*establecer procedimientos o instituciones jurídicas, administrativas u otras para la protección de la intimidad y de las libertades individuales respecto a los datos personales*». En particular, las Directrices se refieren a la adopción de «*legislación nacionales adecuadas*», «*fomentar y apoyar la autorregulación*» y la adopción de «*códigos de conducta*», «*prever medios razonables para que las personas ejerciten sus derechos*», «*prever las sanciones y recursos suficientes en caso de incumplimiento de las medidas con las cuales se implanten los principios expuestos en las Partes II y III*», en fin, «*asegurar que no haya discriminación injusta contra los sujetos de los datos*»[98]. Sin embargo, debe destacarse que las Directrices no hacen en ningún momento referencia a la creación de autoridades nacionales de protección de datos personales, sino que únicamente impulsan la adopción de medidas nacionales de desarrollo de éstas.

69. Aunque las Directrices no son vinculantes para los Estados miembros de la OCDE, sus principios básicos de privacidad han influido mucho en la elaboración de leyes y normas sobre privacidad de datos en Europa (Consejo de Europa y UE) y en jurisdicciones no europeas como Australia, Nueva Zelandia Zelanda y Canadá. Además, constituyeron un punto de partida para la adopción del "Marco de Privacidad" (*APEC Privacy Framework*)[99].

---

[96] Emilia ZABALLOS PULIDO (2013: 93). GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1998), *Documento de Trabajo - Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*, aprobado por el Grupo de Trabajo el 24 de julio de 1998, WP 12. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf [consulta: 05 de diciembre de 2015].

[97] DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 6-7).

[98] DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 6).

[99] La APEC, creado en 1989, es un foro económico que reúne a 21 países de las áreas de Asia y del Pacífico, con el fin de consolidar el crecimiento y la prosperidad de los países del Pacífico, que trata temas relacionados con el intercambio comercial, coordinación económica y cooperación entre sus integrantes. Alineándose con las Directrices de la OCDE, en 2004 los Ministros del Área APEC, reconociendo la importancia de la protección de la privacidad y que ésta pudiera ser obstáculo al flujo de información, aprobaron un "Marco de Privacidad" (*APEC Privacy Framework*), con el ánimo de impulsar la apropiada protección de la información personal, prevenir la creación de barreras innecesarias al flujo de información, promover que empresas multinacionales

Todos estos instrumentos, que reflejaban el principio básico de las Directrices de la OCDE, aumentaron la importancia jurídica del principio, especialmente cuando la Directiva de la UE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos se adoptó quince años después[100].

70. Las Directrices de la OCDE, por otra parte, se consideran como el «*primer texto que establece de una forma sistemática los principios fundamentales del derecho a la protección de los datos de carácter personal*»[101]. Ellas anticiparon los tiempos, convirtiéndose en lo que serían los principios fundamentales en materia de protección de datos. Sin embargo, ellas se propusieron un objetivo modesto: «*Estas Directrices deberían considerarse como criterios mínimos susceptibles de suplementarse con medidas adicionales para la protección de la intimidad y las libertades individuales*»[102], dentro de los países adherentes.

71. Las Directrices, establecidas en 1980, han resistido mucho al impacto del tiempo, gracias a su formulación tecnológicamente neutral, apartada de referencias técnicas específicas, que las hacía susceptibles a aplicarse también a las nuevas tecnologías.

72. Las Directrices de 1980 se complementan con la adopción, el 26 de noviembre de 1992, de la Recomendación del Consejo OCDE concerniente a las Directrices de Seguridad de los Sistemas de Información, la cual se encuentra más enfocada hacia cuestiones económicas y legales relativas a las transmisiones internacionales de datos, telecomunicaciones y servicios[103]. Tras de los atentados a Estados Unidos del 11 de

utilicen métodos uniformes para recabar y procesar datos personales, y facilitar esfuerzos nacionales e internacionales para exigir la protección de datos personales. Para mayores detalles, véase APEC Privacy Framework, accesible en Internet: http://publications.apec.org/publication-detail.php?pub_id=390 [consulta: 07 de diciembre de 2015].

[100] Avner LEVIN and Mary JO NICHOLSON (2005: 375).

[101] Emilia ZABALLOS PULIDO (2013: 93).

[102] Apartado 6 de las DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES (1980: 4).

[103] «*El 11 de abril de 1985 los ministros de la OCDE adoptaron la "Declaración sobre flujos de datos transfronterizos". Esta declaración abordaba las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intra-empresariales, servicios de información informatizada, e intercambios científicos y tecnológicos. Al adoptar esta declaración, los gobiernos de la OCDE reafirmaron su compromiso por desarrollar enfoques comunes ante las cuestiones de flujos de datos transfronterizos y, si se presentara la ocasión, desarrollar soluciones armonizadas. Esta publicación incluye la "Declaración sobre flujos de datos transfronterizos"*». En la conferencia ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en 1998 en Ottawa, los ministros reafirmaron «*su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales*». Declararon concretamente que «*trabajarían para vincular los diferentes enfoques adoptados por los países miembros con vistas a asegurar la protección de la privacidad en las redes globales basándose en las directrices de privacidad de la OCDE*». Durante dicha conferencia, los ministros adoptaron una declaración

septiembre, el Comité de Política de Información, Informática y Comunicaciones de la OCDE para promover la implantación de estas Directrices, acometió en el 2001 la revisión de las Directrices sobre seguridad de 1992 (revisada en 1997) al Grupo de expertos de Seguridad de la Información y Protección de la Privacidad (WPISP). Se adoptaron como Recomendación del Consejo de la OCDE el 25 de julio de 2002, que viene a reemplazar a la Recomendación del Consejo concerniente a las Directrices de Seguridad de los Sistemas de Información del 26 de noviembre de 1992[104].

3.2. Recomendación revisada sobre las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales 2013

73. En 2011 se reunió el Grupo de expertos de Seguridad de la Información y Protección de la Privacidad (WPISP) para comparar la situación de aquel momento con la de los años 80, constatando cambios profundos en el valor de los datos personales en la economía, en la sociedad actual y por tanto en nuestras vidas. Cambios tales como el volumen de datos de carácter personal que se recogen, usan y almacenan; los distintos tipos de análisis de datos que pueden proporcionar perfiles de individuos o grupos; los beneficios sociales y económicos que se obtienen con los nuevos usos y las nuevas tecnologías; la magnitud de las amenazas a la privacidad; la cantidad de actores que intervienen pudiendo poner en riesgos la protección de la privacidad; la frecuencia y complejidad de las interactuaciones

que reafirmaba su compromiso sobre la protección de la privacidad en las redes globales y el inicio de acciones para futuros trabajos en este sentido. Esta publicación incluye también la Declaración ministerial sobre la protección de la privacidad en las redes globales. *Vid*. «Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales», en *OCDE Online Bookshop*, 2002, pág. 3. Disponible en internet: http://www.oecd.org/sti/ieconomy/15590267.pdf [consulta: 07 de diciembre de 2015].

[104] DIRECTRICES DE LA OCDE PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD, adoptados como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002, págs. 12. Disponible en internet: https://www.oecd.org/sti/ieconomy/34912912.pdf [consulta: 07 de diciembre de 2015]. Estas Directrices «*pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad – esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información. Estas Directrices marcan una clara ruptura con un tiempo en el que los aspectos de seguridad y el uso de redes y sistemas se consideraban con frecuencia como elementos a posteriori. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proporcionar una seguridad efectiva. Cada participante es un actor importante en la garantía de la seguridad. Cada participante de acuerdo con el papel que desempeña deberá ser consciente de los riesgos de seguridad y de las medidas preventivas que sean oportunas, debiendo asumir la responsabilidad que les corresponde y tomar las medidas necesarias para fortalecer la seguridad de los sistemas y redes de información*». DIRECTRICES DE LA OCDE PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD, págs. 6-8.

personales y la disponibilidad global de datos de carácter personal, el apoyo de redes y plataformas que permiten el continuo flujo de datos[105].

74. El 11 de julio de 2013, el Consejo de la OCDE adoptó una Recomendación revisada respecto de las Directrices sobre la Privacidad de 1980, cuyo objetivo es adaptar los principios establecidos en la experiencia pasada a los retos actuales, conscientes de la dimensión cada vez más global asumida por la cuestión de la protección de datos personales[106]. Se pueden apreciar cambios significativos en dos niveles: por un lado, se aboga por un enfoque basado en la gestión de riesgos, para la aplicación práctica de la protección de la privacidad; por otro, destaca la profusión de un mayor compromiso por parte de los Estados miembros en la mejora de la interoperabilidad.

75. En el primer caso, se introducen nuevas disposiciones, centradas en la persona responsable del tratamiento de datos personales. Nos referimos al principio de responsabilidad o rendición de cuentas -"*accountability*" en inglés-, lo cual supone que los responsables del tratamiento adopten programas efectivos de cumplimiento de la normativa para poder gestionar mejor el riesgo, que se refiere como "programas de gestión de la privacidad". Este principio también se reconoce en el nuevo Reglamento General de Protección de Datos de 2016, especialmente en el artículo 5, apartado 2, en el que el responsable del tratamiento será responsable del cumplimiento de los principios relativos al tratamiento y capaz de demostrarlo («*responsabilidad proactiva*») (*vid. amplius*, Capítulo V). Se trata, por tanto, de que se establezcan "puertos seguros" en las organizaciones, que permitan gestionar el riesgo que supone y conlleva todo tratamiento de datos personales[107]. En particular, se hace hincapié en la necesidad de que el responsable del tratamiento de datos se dote de mecanismos que le permitan responder sin demora a las demandas de los interesados y proceder con prontitud para notificar a la autoridad de supervisión o de otras autoridades competentes en caso de cualquier violación a la seguridad de los datos personales: la notificación de las brechas de seguridad, tanto a una autoridad de control como

[105] María Belén SÁNCHEZ GONZÁLEZ (2016), *Implicaciones institucionales de la ley de Protección de Datos*, Tesis doctoral, Universidad de Málaga, pág. 52. Disponible en Internet: http://riuma.uma.es/xmlui/handle/10630/11792 [consulta: 20 de mayo de 2017].
[106] RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], págs. 11-37. Disponible en internet: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [consulta: 08 de diciembre de 2015].
[107] Miguel RECIO (2013), «La OCDE actualiza sus directrices sobre protección de datos», en *Lawyerpress*, 12 de septiembre.

a los sujetos afectados, reforzando así el deber de seguridad que es clave para garantizar la protección de datos personales[108].

76. Las pautas de privacidad de 2013 resaltaron que los responsables del tratamiento tienen un papel importante para que la protección de datos funcione en la práctica. Las Directrices comprenden un principio de rendición de cuentas en el sentido de que un responsable de datos debe ser responsable de cumplir con las medidas que dan efecto a los principios "materiales" establecidos[109].

77. El cumplimiento (en inglés, "*enforcement*") es otro de los aspectos a los que presta atención la OCDE, siendo la primera vez que las Directrices se refieren a las autoridades de protección de datos ("*privacy enforcement authorities*"). Hemos de resaltar aquí que es la primera vez que la OCDE reconoce las Autoridades de control[110], como un organismo público establecido por cada país miembro y que será responsable del cumplimiento de la normativa de protección de datos, a las que les reconoce el poder de investigar, así como de ejecutar las normas[111].

78. La segunda cuestión también relevante en estas Directrices es el aumento de los compromisos que los Estados miembros están llamados a asumir, desarrollando estrategias nacionales de privacidad que reflejen un enfoque coordinado entre los organismos

[108] Véase, por ejemplo, apartado 15, introducido *ex novo*: «*A data controller should: a) Have in place a privacy management programme that: i. gives effect to these Guidelines for all personal data under its control; ii. is tailored to the structure, scale, volume and sensitivity of its operations; iii. provides for appropriate safeguards based on privacy risk assessment; iv. is integrated into its governance structure and establishes internal oversight mechanisms; v. includes plans for responding to inquiries and incidents; vi. is updated in light of ongoing monitoring and periodic assessment; b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects*». RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 16).

[109] RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 15-16).

[110] Al respecto, la OCDE ha sido la impulsora de la Red Global de Autoridades de Protección de Datos ("*Global Privacy Enforcement Network*"), en la que participa la Agencia Española de Protección de Datos y para Italia el Garante per la Protezione dei Dati Personali. Global Privacy Enforcement Network, accesible en: https://www.privacyenforcement.net/ [consulta: 08 de diciembre de 2015]. Miguel RECIO (2013).

[111] Se recoge la definición en el punto 1 d) de la parte primera del Anexo de las Directrices para la protección de la privacidad y la transferencia de datos personales de 2013: «*"Privacy enforcement authority" means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings*». RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 13).

gubernamentales ("estrategia nacional de privacidad"). Se introduce, en este sentido, un nuevo concepto, orientado a asegurar que las autoridades nacionales ejerciten más esfuerzos hacia una mayor coordinación en su interior, incluso más que entre sí. Puesto que el control independiente ha demostrado ser esencial para el desarrollo de la protección de datos eficaz, una nueva disposición se introdujo en las Directrices de 2013, que insta a los países miembros a establecer y mantener las autoridades encargadas de la aplicación de la legislación en materia de privacidad con la gobernanza, los recursos y los conocimientos técnicos necesarios para ejercer sus competencias con eficacia y para tomar decisiones sobre una base objetiva, imparcial y coherente[112].

79. En este sentido, se enfatiza que los Estados deben potenciar y compartir profundamente, a través de iniciativas de formación específicas y programas para la adquisición de un mínimo de conocimientos técnicos, y de que sólo una mejor comprensión de los riesgos permite una mejor protección de la privacidad, y que estas competencias no sea de solo dominio de unas pocas personas expertas[113]. Es decir, es el impulso de políticas públicas por lo que se refiere al cumplimiento a nivel nacional, lo que las puede hacer efectivas. Por fin, no se trata sólo de adoptar medidas legislativas, sino de impulsar también la cultura en materia de protección de datos y privacidad.

80. En cuanto a las transferencias internacionales, las Directrices hacen especial énfasis a la importancia del flujo transfronterizo de datos por ser fuente de progreso y economía, y asumen y se adaptan a la nueva realidad del "*cloud computing*"[114]. Por ello la OCDE, en aras a facilitar el flujo internacional de los datos, incide sobre la responsabilidad ("*accountability*") del responsable del tratamiento, con independencia de que éste se

[112] Part Five. National Implementation, apartado 19: «*In implementing these Guidelines, Member countries should: a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies; b) adopt laws protecting privacy; c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis* (…)». RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 17).

[113] Part Five. National Implementation, apartado 19: «(…) *d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise; e) provide for reasonable means for individuals to exercise their rights; f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy; g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy; h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and i) ensure that there is no unfair discrimination against data subjects*». RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 17).

[114] RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 29 y ss).

encuentre en un modelo basado en el "nivel adecuado" (de protección) de un país o en el uso de medidas tales como las normas corporativas vinculantes (*Binding Corporate Rules - BCRs*)[115] o las reglas de privacidad transfronterizas (*Cross-Border Privacy Rules - CBPRs*)[116].

81. La elección de realizar una revisión de las Directrices de 1980, conservando la estructura original con respecto a los principios básicos de la materia, ha sido oportuna, pero siguen existiendo, sin embargo, dos límites importantes. En primer lugar, las Directrices, instrumentos de derecho blando ("*soft law*"), no imponen a los Estados miembros una obligación vinculante y ejecutable para transponer a la legislación nacional[117], aunque las *Guidelines* tuvieron el mérito de plantear ciertos principios que fueron puntos de referencia reales para las reglas y procedimientos elaborados con posterioridad en relación con el tratamiento y transferencia transfronterizo de datos personales. Además, tienen una vocación principalmente comercial: están orientados a la eliminación de barreras injustificadas al movimiento transfronterizo de datos y al desarrollo de las relaciones económicas y sociales entre los Estados miembros de la OCDE, mientras que parece que el perfil de la protección de los derechos individuales se ve ensombrecido[118].

82. A pesar de la naturaleza de las normas de las Directrices, sin embargo, en las líneas anteriormente descritas, como se ha apuntado, el nuevo Reglamento General de Protección de Datos incorpora también estos nuevos principios y está en conformidad con las Directrices de la OCDE.

83. También, los principios descritos en estas Directrices (consentimiento, información, control, calidad, lealtad, seguridad y confidencialidad) coinciden plenamente, como veremos

[115] Véase más detalle, Capítulos IV y V.
[116] Las Reglas Transfronterizas de Privacidad (CBPR) es un sistema de reglas acerca de la privacidad en el flujo transfronterizo de datos en el área de la APEC. *Amplius vid*., http://www.cbprs.org/GeneralPages/About.aspx. María Belén SÁNCHEZ GONZÁLEZ (2016: 54).
[117] Interesante la opinión crítica de Alfonso Ortega Giménez sobre las iniciativas que emanan de organizaciones intergubernamentales de alcance global estudiadas aquí: «*son claramente insuficientes para garantizar el derecho a la protección de datos de carácter personal. Las normas emanadas de estas instancias internacionales o bien no son directamente invocables por los particulares (perjudicados) o bien carecen de una traducción adecuada al plano práctico. El titular del derecho a la protección de datos sigue encontrándose en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección*». *Vid*. Alfonso ORTEGA GIMÉNEZ (2015: 43).
[118] *Vid*. RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013: 12): «*to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them*».

más adelante, con el contenido del derecho fundamental recogido en los distintos instrumentos europeos, tales como el Convenio n. 108 del Consejo de Europa, la Carta de Derecho Fundamentales de la Unión Europea o la Directiva 95/46/CE.

4. Limitaciones del derecho fundamental de la privacidad en nombre de la seguridad en el Consejo de Europa

84. Siguiendo el marco normativo actualmente aplicable a la protección de datos personales en Europa, esencialmente «*tenemos que recurrir, por una parte, al proceso evolutivo que ha sufrido este derecho fundamental, y por otra, hacer mención de las diversas fuentes de las cuales proviene su regulación. De esta forma se comprende la superposición de normas, tanto supranacionales provenientes de los convenios del Consejo de Europa como de las normas emanadas de las diversas fases del proceso de consolidación de la Unión*»[119]. Es por ello por lo que los apartados siguientes recogen los documentos legislativos presentes en materia de protección de datos proveniente por el Consejo de Europa y su Tribunal.

85. En Europa, el interés por el derecho a la privacidad aumentó con el fin de la Segunda Guerra Mundial, que generó un marco alto de sensibilidad en el tema de la protección de la esfera de la intimidad tratado inicialmente por el Consejo de Europa (en adelante, CdE)[120]. Sin embargo, entre los años 1960 y 1970 con el advenimiento de las tecnologías de la información y el potencial de vigilancia de los sistemas informáticos de gran alcance, se

[119] Alejandro Luis GACITÚA ESPÓSITO (2014: 124).

[120] El Consejo de Europa, con sede en Estrasburgo (Francia), reúne en la actualidad, con sus 47 estados miembros, a casi todos los países del continente europeo. El Consejo de Europa nació el 5 de mayo de 1949 tras la firma de su Carta fundacional -el Tratado de Londres- por parte de Bélgica, Francia, Luxemburgo, Países Bajos y Reino Unido. Poco después, se adhirieron Irlanda, Italia, Dinamarca, Noruega y Suecia. El Consejo de Europa tiene como objetivo fomentar la creación de un espacio democrático y jurídico común, para garantizar el respeto de los principios fundamentales: los derechos humanos, la democracia y el Estado de Derecho, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales y otros textos de referencia de referencia relativa a la tutela del individuo. *Vid*. *amplius*, José María SIERRA NAVA (1957), *El Consejo de Europa*, Madrid, Instituto de Estudios Políticos, págs. 335; Manuel DIEZ DE VELASCO (2010), *Las organizaciones internacionales*, 16ª ed., Madrid, Tecnos, págs. 952; Francisco José MONTES FERNÁNDEZ (2014), «El Consejo de Europa», en *Anuario Jurídico y Económico Escurialense*, núm. 47, págs. 57-92. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=4639615 [consulta: 15 de julio de 2015]. Pueden consultarse la página web del Consejo de Europa, disponible en: http://www.coe.int/en/web/portal/home.

impulsó la demanda de normas específicas para regular la obtención y manejo de información personal[121].

86. Por parte del Consejo existía conciencia de las «*potenciales amenazas que representaba el procesamiento de datos personales a través de medios informáticos para la vida privada de los sujetos*»[122]. Esta preocupación sobre la regulación de los datos de carácter personal, añadida a la de proporcionar una protección a la privacidad de los individuos, respondía a «*la necesidad de dar claridad y certeza jurídica respecto del tráfico internacional de datos personales*»[123]. Se buscaba ya desde entonces «*facilitar el intercambio de datos y las relaciones institucionales y comerciales entre los distintos países, evitando los paraísos de datos*»[124].

87. Son dos los instrumentos internacionales del Consejo de Europa que han tenido «*mayor impacto en el desarrollo del derecho a la protección de datos*»[125]: el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950 (en adelante, CEDH), conocido también como el Convenio de Roma de 1950, que establece por primera vez a nivel europeo la tutela de la vida privada; y el Convenio n. 108 del Consejo de Europa para la protección de las persones con respecto al tratamiento automatizado de datos de carácter personal, «*que define desde una perspectiva normativa el contexto de protección de la privacidad en relación con las TIC*»[126].

88. Analizaremos que el derecho a la privacidad y de los datos personales están garantizados tanto por los convenios del CdE como por la actividad interpretativa de su Tribunal (Tribunal Europeo de Derechos Humanos - TEDH, también conocido como

[121] En el 1967, se constituyó en el seno del CdE una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a no sufrir injerencias en la vida privada, y de ella surgió la Resolución 509/1968 de la Asamblea del Consejo Europa sobre "Los Derechos humanos y los nuevos logros científicos y técnicos", que se considera el origen del movimiento legislativo que desde entonces recorrerá Europa en materia de protección de datos. La citada Resolución, si bien no menciona la protección de datos directamente, concreta la necesidad de adoptar mecanismos de protección que comprenda la vida privada y otros derechos fundamentales que pueden verse afectados por las TIC (Tecnologías de la información y la comunicación). *Vid*. Cristina ALMUZARA ALMAIDA (coord.), Fanny COUDERT, Ana MARZO PORTERA, Yolanda NAVALPOTRO (2007), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed., Valladolid, Lex Nova, págs. 33 y ss.
[122] Alejandro Luis GACITÚA ESPÓSITO (2014: 126).
[123] Alejandro Luis GACITÚA ESPÓSITO (2014: 126).
[124] *Vid*. Alejandro Luis GACITÚA ESPÓSITO (2014: 126) y también Antonio TRONCOSO REIGADA (2010), *La protección de datos personales: en busca del equilibrio*, Valencia, Tirant lo Blanch, pág. 56.
[125] Alejandro Luis GACITÚA ESPÓSITO (2014: 126).
[126] Alejandro Luis GACITÚA ESPÓSITO (2014: 127).

Tribunal de Estrasburgo)[127], que en numerosas ocasiones, ha examinado denuncias planteadas en materia de protección de datos, tales como las violaciones a la privacidad producidas por injerencias de las autoridades estatales o, por ejemplo, las injerencias en la vida privada por acceso a datos médicos.

89. También en el espacio específico del tratamiento de datos personales por parte de las autoridades policiales, recordamos que el CdE ha propuesto a los Estados miembros la Recomendación R (87) 15 del Comité de Ministros, para regular la utilización de datos de carácter personal en el sector de la policía. Como analizaremos, en síntesis, dicha Recomendación ha sido referenciada por todas las normas desarrolladas por la Unión Europa respecto al ámbito específico del tratamiento de datos con fines de represión y prevención penal[128].

90. En fin, podemos decir que, en el marco específico de la protección de datos personales, «*la labor desarrollada por el Consejo de Europa puede ser calificada de fundadora*»[129].

[127] El Tribunal Europeo de Derechos Humanos, con sede en Estrasburgo, se creó en 1959. Su jurisprudencia en los últimos años ha podido aclarar muchos aspectos relacionados con la interpretación del derecho fundamental al respeto de la vida privada consagrado en el artículo 8 del CEDH. Al respecto, *vid*. Carlos RUIZ MIGUEL (1994), *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Madrid, Civitas, págs. 134. Disponible en Internet: http://www.academia.edu/25472780/El_derecho_a_la_protecci%C3%B3n_de_la_vida_privada_en_la_jurisprudencia_del_Tribunal_Europeo_de_Derechos_Humanos [consulta: 24 de mayo de 2017]; Mónica ARENAS RAMIRO (2006: 54-86); Xabier ARZOZ SANTIESTEBAN (2009), «Artículo 8: derecho al respeto de la vida privada y familiar», en Iñaki LASAGABASTER HERRARTE (dir.), *Convenio Europeo de Derechos Humanos. Comentario sistemático*, 2ª ed., Madrid, Civitas, págs. 949; Carmen MORTE GÓMEZ y Guillem CANO PALOMARES (2010), «La interpretación evolutiva y dinámica del Convenio Europeo de Derechos Humanos en la jurisprudencia reciente del Tribunal de Estrasburgo», en *Revista General de Derecho Constitucional*, núm. 10, págs. 31. Pueden consultarse también la página web del Tribunal Europeo de Derechos Humanos, disponible en: http://www.echr.coe.int/Pages/home.aspx?p=home&c= [consulta: 01 de diciembre de 2015].

[128] Incluso en la Propuesta de Directiva del Parlamento Europeo y del Consejo de 2012, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, se hace referencia en los motivos a esta Recomendación del Consejo de Europa (*vid*. *infra*).

[129] Alejandro Luis GACITÚA ESPÓSITO (2014: 125).

4.1. La insuficiente protección de la privacidad por el artículo 8 del CEDH. El estado de emergencia y el Estado de Derecho

91. En el espacio de la Unión Europea, el derecho a la privacidad está protegido principalmente por el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950 (CEDH)[130] y por la actividad hermenéutica del TEDH.

92. Desde esta actividad conjunta, el Convenio penetró en las tradiciones jurídicas de los Estados del CdE, estableciendo una base legal común para todos ellos[131]. Al igual que otros instrumentos protectores de los derechos humanos de la ONU, nace y se inspira a partir de la DUDH de 1948, y establece los criterios jurídicos precisos de la protección del derecho a la intimidad. No obstante, y habiendo tenido de referente la DUDH, «*el Convenio de Roma se presenta con un contenido material mucho menor*»[132].

93. Este Convenio internacional «*de carácter regional contiene un catálogo de derechos y libertades fundamentales que los Estados firmantes se comprometen a respetar y garantizar*»[133]. La mayoría de los países que se han adherido al Tratado, han incorporado sus disposiciones dentro del propio sistema jurídico, por lo que también se puede invocar el Convenio ante los tribunales nacionales. Así pues, el CEDH es el primer instrumento jurídico internacional para la tutela de los derechos, que reconoce por primera vez la privacidad como un derecho humano, más precisamente como un derecho humano fundamental[134].

---

[130] CONVENIO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES, Roma, 4.XI.1950. La preocupación por la protección del derecho a la intimidad expresa la voluntad general, después de la Segunda Guerra Mundial, para borrar los crímenes y atentados contra la dignidad humana, el establecimiento de un sistema completo de normas para garantizar futuros abusos. Es importante destacar, en este sentido, el Convenio de 1950, que entró en vigor en 1953, en el artículo 8 reconoce que cada persona tiene derecho al respeto de su vida privada y familiar.

[131] El Convenio ha sido ratificado por los 47 Estados miembros del Consejo de Europa. Sobre el CEDH hay mucha bibliografía, entre otros, *vid*. Juan Antonio CARRILLO SALCEDO (2004), *El Convenio Europeo de Derechos Humanos*, Madrid, Tecnos, págs. 160; Alastair MOWBRAY (2012), *Cases, Materials, and Commentary on the European Convention on Human Rights*, 2ª ed., Oxford, Oxford University Press, págs. 936; Christopher KUNER, (2013), *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, págs. 312; Bernadette RAINEY, Elizabeth WICKS, and Clare OVEY (2014), *Jacobs, White and Ovey: The European Convention on Human Rights*, 6ª ed., Oxford, Oxford University Press, págs. 728; David HARRIS, Michael O'BOYLE, Edward BATES, and Carla BUCKLEY (2014), *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights*, 3ª ed., Oxford, Oxford University Press, págs. 1080; William A. SCHABAS (2015), *The European Convention on Human Rights*, Oxford, Oxford University Press, págs. 1440.

[132] Luis Antonio ANGUITA VILLANUEVA (2004), «La cultura en la Carta de los Derechos Fundamentales de la Unión Europea», en Carlos RUÍZ MIGUEL (coord.), *Estudio sobre la Carta de los derechos fundamentales de la Unión Europea*, Santiago de Compostela, Universidad de Santiago de Compostela, pág. 93.

[133] Alejandro Luis GACITÚA ESPÓSITO (2014: 127).

[134] Por su parte, el CEDH se inspira en otros documentos internacionales de derechos, como se nota en su considerando, directamente en la DUDH de 1948, introdujo el artículo 5 (Derecho a la libertad y a la seguridad), y en el Pacto Internacional de Derechos Civiles y Políticos (*vid*. *supra*). Sin embargo, existen importantes

94. La protección de la privacidad y de los datos personales comienza a afirmarse a través de la lectura exegética formada por el TEDH sobre del artículo 8 del CEDH, que protege el derecho a la intimidad y familiar, así como su correspondencia y el domicilio[135], a pesar de no tener un contenido de dicha disposición específicamente dedicada a las cuestiones mencionadas. No hay mucha evidencia sobre lo que los redactores del Convenio entendían por el término "privacidad" o "vida privada", ya que apenas existen registros de discusiones sobre asuntos fundamentales, como los aspectos de privacidad[136]. Por consiguiente, el TEDH ha intentado dar una explicación general en numerosas decisiones sobre el alcance de la protección de la vida privada en lo que se refiere a la interferencia en las comunicaciones electrónicas. Los juicios históricos del Tribunal han involucrado actividades estatales en las áreas sensibles de la ley y la práctica de la seguridad nacional. El Tribunal no ha dudado en afirmar que las actividades de vigilancia constituyen una injerencia en el respeto de la vida privada (sobre la jurisprudencia del TEDH, *vid*. *infra*).

95. Con una formulación afirmativa en su primer apartado, el artículo 8 (Derecho al respeto a la vida privada y familiar) reconoce que «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*»; luego continúa, reproduciendo de manera más circunstanciada la prescripción negativa sobre la prohibición de la interferencia en la esfera privada ya presente en las fuentes internacionales[137]: «*No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*».

96. La norma, por lo tanto, tiene una estructura dual: en el primer apartado, reconoce el carácter de universalidad de los derechos humanos, y cómo el derecho a la privacidad hace

diferencias: el CEDH es un Tratado internacional y, como tal, es obligatorio, en cambio la DUDH carece de obligatoriedad; el CEDH reconoce un sistema de garantías judiciales internacionales para verificar el cumplimiento de los derechos reconocidos en el Convenio y que la DUDH ni siquiera establece.

[135] Orla LYNSKEY (2014), «Deconstructing data protection: the 'Added-value' of a right to data protection in the EU legal order», en *International and Comparative Law Quarterly*, núm. 63, vol. 3, págs. 569-597. Disponible en Internet: http://eprints.lse.ac.uk/57713/ [consulta: 11 de diciembre de 2015]. El artículo 8 del CEDH, sigue de cerca los artículos 12 de la DUDH y 17 del PIDCP. También véanse Oliver DIGGELMANN and Maria Nicole CLEIS (2014: 452).

[136] Oliver DIGGELMANN and Maria Nicole CLEIS (2014: 457).

[137] *Vid*. *supra*.

referencia a los titulares de esos derechos, es decir, al carácter universal de "toda persona" al respeto de su vida privada y familiar, de su domicilio y de su correspondencia[138]. Por ello, los ciudadanos europeos que han visto vulnerada su privacidad en los casos de violación sí que encuentran su vida privada protegida por dicho Convenio.

97. Al tiempo, analizando el segundo apartado, se identifican las excepciones admisibles y se establecen las condiciones en las que legítimamente pueden imponerse restricciones al derecho al respeto de la vida privada: se regula la injerencia de las autoridades públicas, limitándola a los específicos casos detallados. En este sentido, se permite una compresión del derecho al respeto a la vida privada y familiar sólo sobre la base de tipos de supuestos sucintamente reconocidos en el CEDH, si bien especificados y desarrollados a través de diversas resoluciones del Tribunal de Estrasburgo.

98. Según el mismo apartado, la «*injerencia*» por parte del Estado debe ser prescrita por ley (principio de legalidad) y ser necesaria con el fin de garantizar la "seguridad nacional o pública", "el bienestar económico del país", "la defensa del orden y la prevención del delito", "la protección de la salud o de la moral", así como "la protección de los derechos y libertades de los demás", en el marco de una sociedad democrática[139].

99. Siguiendo abajo las excepciones admisibles, la vaguedad de la formulación del artículo 8 tiende a debilitar el alcance del reconocimiento y la protección del derecho a la privacidad. De hecho, parece que en el apartado 2 la prevalencia de los derechos y libertades de los demás, no especificados, sobre el derecho a la privacidad, legitima un predominio por parte de la autoridad pública. En consecuencia, si en general sobre el Estado hay la obligación de abstenerse de interferir en la vida privada y familiar de los ciudadanos, las únicas medidas restrictivas permitidas por los jueces de Estrasburgo son las comprendidos dentro de un "margen de apreciación nacional"[140]: es decir, las intervenciones previstas por

[138] José Luis PÉREZ TRIVIÑO (1995), «Derechos humanos, relativismo y protección jurídica de la moral en el Convenio Europeo de Derechos Humanos», en *Doxa. Cuadernos de Filosofía del Derecho*, núm. 17-18, págs. 470 y ss. Disponible en Internet: http://www.cervantesvirtual.com/obra/derechos-humanos-relativismo-y-proteccin-jurdica-de-la-moral-en-el-convenio-europeo-de-derechos-humanos-0/ [consulta: 11 de mayo de 2017].

[139] Artículo 8 (Derecho al respeto a la vida privada y familiar) del CEDH; Ugo PAGALLO (2014), *Il diritto nell'età dell'informazione*, Torino, G. Giappichelli Editore, págs. 165. Disponible en Internet: http://it.scribd.com/doc/251335183/Il-diritto-nell-eta-dell-informazione-U-Pagallo-2014#scribd [consulta: 20 de marzo de 2016].

[140] El llamado "margen de apreciación nacional" es una doctrina de consecuencias muy importantes y que ocupa un lugar central en la jurisprudencia de Estrasburgo, pero cuya aplicación práctica y construcción teórica tienen contornos altamente discrecionales e imprecisos y, en consecuencia, no por ser una jurisprudencia necesaria, resulta menos controvertida. En Francisco Javier GARCÍA ROCA (2007), «La muy discrecional

la ley en el Estado que, en cambio, se materializan en medidas necesarias en una sociedad democrática para perseguir intereses colectivos o individuales[141]. Esto es perceptible en el juicio de proporcionalidad[142], que se convierte en un factor destacado en la protección de los datos personales en Europa, lo que representa un parámetro importante para determinar la interferencia legítima en la vida privada de una persona. Este principio y su aplicación son, a causa de la sensibilidad de los datos recogidos y los fines para los que se utilizan en el ámbito en cuestión, aún más importante en el Espacio de libertad, seguridad y justicia[143].

100. En definitiva, una acción estatal invasiva de la privacidad individual es legítima sólo cuando hay tres hipótesis: 1) prevista y conforme a la ley; 2) dirigida a conseguir un objetivo digno de protección (la defensa del orden público); y 3) que resulta adecuada para alcanzar el objetivo perseguido. Las medidas restrictivas aplicadas, sin embargo, siempre deben mantener el carácter de temporalidad sin dar lugar a restricciones indeterminadas, que afecten a los derechos individuales, en especial modo a la vida privada[144].

101. A pesar del papel crucial desempeñado por el artículo 8 del CEDH, el mismo se caracteriza por un ámbito de aplicación particularmente amplio, para cubrir situaciones jurídicas y de hecho bastante heterogéneas. En efecto, se reconoce expresamente el interés de cada persona respeto de la misma vida privada y familiar y, como indicamos, no define precisamente la noción. En relación específica al concepto de "vida privada", el TEDH se ha expresado, en repetidas ocasiones, sobre este término amplio no susceptible de definición exhaustiva: «*Private life is a broad term not susceptible to exhaustive definition*»[145]. Esto permitió a los jueces de Estrasburgo identificar los perfiles legalmente relevantes del concepto de privacidad, operando un equilibrio con los intereses contrapuestos y teniendo en cuenta las nuevas necesidades de protección que surjan en relación a las tecnologías en

doctrina del margen de apreciación nacional según el Tribunal Europeo de Derechos Humanos: soberanía e integración», en *UNED. Teoría y Realidad Constitucional*, núm. 20, pág. 118. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2520040 [consulta: 25 de febrero de 2016].

[141] Entre ellos: la seguridad nacional, el orden público, el bienestar económico, la prevención de actos delictivos, la protección de los derechos y libertades de los demás.

[142] Francisco Javier GARCÍA ROCA (2007: 121 y ss.).

[143] Beatriz S. TOMÁS MALLÉN (2014), «Privacidad versus seguridad en el ámbito europeo», en Antonio FAYOS GARDÓ (coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, Librería-Editorial Dykinson, págs. 236 y ss. Sobre el ELSJ, interesante la investigación de Esther M. ANÍBARRO MARTÍNEZ (2016), *El espacio de libertad, seguridad y justicia en la Unión Europea: proyecto jurídico-político "In Fieri"*, Tesis Doctoral, Valladolid, Universidad de Valladolid Instituto de Estudios Europeos, págs. 625.

[144] En este sentido, *vid*. más adelante los casos jurisprudenciales del Tribunal como: *Leander contra Suecia*, apartado 59; *Klass y otros contra Alemania*, apartado 42; y *Rotaru contra Romania* [GS], apartado 47.

[145] *Vid*. Bernadette RAINEY, Elizabeth WICKS, and Clare OVEY (2014: 362); Philip COPPEL (2014), *Information Rights: Law and Practice*, 4ª ed., Oxford, Hart Publishing, págs. 827.

evolución. En consecuencia, el Tribunal se refirió al tema al asegurar un marco apropiado del significado y propósito del concepto de "vida privada", contando entre los beneficiarios de la protección otorgada por el artículo 8 del CEDH los diferentes intereses relacionados con el desempeño de la privacidad individual; entre estos, también la protección de datos de carácter personal[146].

102. Por lo tanto, tenemos un instrumento protector que no es diferente de los demás y que se caracteriza porque el máximo Tribunal garante de dicho instrumento se ha pronunciado en favor de una interpretación de tipo *ad hoc* con el tiempo y la sociedad que regula, al considerarlo como un documento vivo, que avanza y evoluciona.

103. En este marco, la posibilidad reconocida en el artículo 8, apartado 2, de "suspender" ciertos derechos a través del uso de la excepción constituye disposición central en la arquitectura del Convenio[147]. No nos parece razonable privar a un Estado a la toma de

[146] Es decir, el artículo 8 del CEDH incluye el derecho al nombre, a la protección de la intimidad y la autonomía personal, así como la libertad de obrar sin interferencia con respecto a su vida privada como la orientación y la vida sexual. Protege, también, el derecho a la identidad y la imagen, existiendo una zona de interacción de la persona con terceros, incluso en un contexto público, que puede entrar en el ámbito de la noción de "vida privada". Por último, también incluye el derecho al desarrollo de las relaciones sociales como una expresión de la realización de su personalidad, y la protección de datos personales. En otras palabras, el respeto a la vida privada no se limita sólo a proteger la integridad moral del individuo, sino también de todas aquellas interferencias, también físicas, que pueden lesionarla. A título de ejemplo el caso *S. and Marper contra Reino Unido* (*infra*), apartado 103: «*The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention*».

[147] En relación del papel limitador que el derecho supranacional puede jugar frente a la acción de los Estados, conviene recordar que algunos instrumentos internacionales de protección de los derechos humanos contienen disposiciones que delinean las excepciones admisibles en tiempos de emergencia pública. De hecho, el artículo 15 (Derogación en caso de estado de excepción), apartado 1, del CEDH permite a los Estados adoptar medidas de excepción de sus obligaciones convencionales «*en caso de guerra o de otro peligro público que amenace la vida de la nación, cualquier Alta Parte Contratante podrá tomar medidas que deroguen las obligaciones previstas en el presente Convenio en la estricta medida en que lo exija la situación, y a condición de que tales medidas no estén en contradicción con las restantes obligaciones que dimanan del derecho internacional*». El TEDH ha considerado contrarias a este precepto algunas medidas adoptadas en el marco del artículo 15 como en los casos: *Lawless contra Irlanda*, de 1 de julio de 1961; *Irlanda contra el Reino Unido*, de 18 de enero de 1978; *Brannigan and McBride contra el Reino Unido*, de 26 de mayo de 1993; *A y otros contra Reino Unido*, de 19 de febrero de 2009. *Vid*. Benedetto CONFORTI (2015), «Francia, lo stato di emergenza e lo stato di diritto», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/articolo.asp?ID=3262 [consulta: 02 de marzo de 2016]; Emanuele SOMMARIO (2016), «Attentati di Parigi: la Francia deroga alla Convenzione Europea dei Diritti dell'Uomo», en *SIDIBlog (blog della Società italiana di diritto internazionale e di Diritto dell'Unione europea)*. Disponible en Internet: http://www.sidiblog.org/2016/01/11/attentati-di-parigi-la-francia-deroga-alla-convenzione-europea-dei-diritti-delluomo/ [consulta: 03 de marzo de 2016]. El artículo 15 se elevó a la crónica, como resultado de los ataques de París de 2015. El gobierno francés notificó al Secretario General del Consejo de Europa, la intención de establecer una excepción a la Convención Europea de Derechos Humanos. El documento sostiene que el País se enfrenta a una "amenaza terrorista duradera" para justificar la aplicación de la ley n. 55-385 de 3 de abril de 1955, que regula el instituto del "*état d'urgence*". Sin embargo, muchas de las medidas citadas podrían dar lugar a restricciones en el disfrute de los derechos individuales incompatibles con las normas establecidas por el CEDH. El gobierno francés, por consiguiente, ha decidido derogar el Tratado, como posibilidad prevista en el artículo 15. Este establece que, en caso de guerra o «*de otro peligro público que*

decisiones en una situación excepcional de crisis suspendiendo o condicionando temporalmente, por ejemplo, algunas de sus obligaciones para erradicar el peligro que lo amenaza. No debería, sin embargo, nunca olvidarse que la razón última de la posibilidad de excepción es la protección de la democracia y, con ella, el Estado de Derecho. En otras palabras, la excepción sólo es admisible en la medida en que sea posible para garantizar un retorno a la normalidad y el pleno disfrute de los derechos humanos. Por tanto, en la lucha contra el terrorismo yihadista, el respeto a los derechos humanos debe ser la base. La respuesta de los gobiernos a dicho fenómeno, que ya no puede ser exclusivamente doméstica, necesita de una cooperación con el resto de los miembros de la Unión y del establecimiento de estrategias comunes. Y, tanto los acuerdos supranacionales que se alcancen en ese ámbito como las decisiones nacionales adoptadas en esa lucha han de tener como límite la consideración de los derechos fundamentales[148].

104. En esta óptica, el control de legalidad por los tribunales es decisiva. Tanto en la esfera nacional como de la UE, los tribunales desempeñan un papel de fiscalización que puede convertirse en una de las mejores garantías para la protección de los derechos fundamentales[149]. De hecho, hay situaciones en las que los derechos individuales están en mayor riesgo de ser violados, y, por lo tanto, requieren un examen más atento por los órganos jurisdiccionales.

amenace la vida de la nación», cualquier Estado contratante podrá tomar las medidas de excepción a las obligaciones del Convenio limitadamente a lo estrictamente necesario para hacer frente a la situación, a condición de que ellas no contrasten con las obligaciones de derecho internacional y con aquellos consiguientes de los artículos 2 (Derecho a la vida), 3 (Prohibición de la tortura y los tratos inhumanos o degradantes) y 4 (Esclavitud) del Convenio. *Vid*. RESERVATIONS AND DECLARATIONS FOR TREATY N.005 - Convention for the Protection of Human Rights and Fundamental Freedoms. Disponible en Internet: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations?p_auth=IRgBNXHj [consulta: 04 de marzo de 2016]; «Valls: "El terrorismo formará parte de nuestro día a día durante mucho tiempo"», en *RTVE.es/EFE*, 17.07.2016. Disponible en Internet: http://www.rtve.es/noticias/20160717/valls-terrorismo-formara-parte-nuestro-dia-dia-durante-mucho-tiempo/1372081.shtml [consulta: 04 de marzo de 2016]; LOI n. 55-385 du 3 avril 1955 relative à l'état d'urgence, Version consolidée au 26 novembre 2015. La ley otorga poderes considerables a las autoridades ejecutivas y administrativas, que se consideran necesarios para atender la emergencia.

[148] *Vid*. Rosario SERRA CRISTÓBAL (2016), «Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común», en *UNED. Teoría y Realidad Constitucional*, núm. 38, pág. 488. Disponible en Internet: http://e-spacio.uned.es/fez/view/bibliuned:TeoriayRealidadConstitucional-2016-38-5075 [consulta: 24 de marzo de 2017].

[149] Para ponderar los intereses de las personas físicas en la protección de privacidad y los intereses de la sociedad en la obtención de datos con el fin de combatir la delincuencia y garantizar la seguridad nacional y pública, uno de los instrumentos que puede servir de límite a los excesos por parte de los gobiernos y legisladores nacionales es el control judicial. Rosario SERRA CRISTÓBAL (2016: 494).

105. Ahora, es interesante hacer hincapié en algunos de los casos más relevantes tratados por el TEDH[150], relativos al ejercicio de privacidad por el artículo 8 del CEDH y vulnerabilidad que el mismo Tribunal ha reconocido en determinadas sentencias.

4.2. La evolución del artículo 8 del CEDH entre equilibrio del interés público a la seguridad y protección de privacidad en las principales jurisprudencias del TEDH

106. Las transgresiones a la privacidad son producidas por injerencias de las autoridades estatales que, aunque se hayan producido en conformidad con el Derecho interno, violan el derecho a la privacidad protegido en el CEDH. El TEDH concluirá cuándo una injerencia se entiende como lícita y cuándo viola los límites recogidos en el apartado segundo del artículo 8 del CEDH[151].

107. Algunos pronunciamientos judiciales que ahora vamos a examinar, tienen el objetivo de poner fin, o de otro modo limitar, a las ambiciones de algunos Estados, estableciendo confines muy específicos a la creciente capacidad de los gobiernos para recopilar informaciones sobre sus ciudadanos para ser utilizados en casos futuros[152]. En este sentido, el TEDH establece límites a la proliferación de las restricciones de las libertades debidas a un fortalecimiento de las políticas de seguridad.

---

[150] Como se sabe, la característica principal de la jurisdicción del TEDH es el hecho de que cualquier persona pueda presentar un recurso en contra los Estados parte del Convenio por presuntas violaciones de éste. Sin entrar en el proceso de funcionamiento del Tribunal, es suficiente observar que los individuos pueden recurrir el TEDH sólo después de agotar todos los recursos internos. Las sentencias del TEDH son vinculantes. Sin embargo, el Tribunal no tiene el poder de anular las decisiones de las autoridades nacionales, pero eso no quiere decir que no tenga influencia ni sea decisivo. En términos legales se dice que se trata de sentencias declarativas y obligatorias. Por eso, la jurisprudencia del Tribunal es sin duda importante para comprender el alcance de la disposición en comentario, así como las cuestiones jurídicas que subyacen a su aplicación práctica. En segundo lugar, porque, dado que la Unión Europea reconoce y garantiza los derechos inviolables del hombre, reconocido por el CEDH, no se puede prescindir de la interpretación de estos derechos por el Tribunal de Estrasburgo. *Vid*. *amplius*, Julia RUILOBA ALVARIÑO (2006), «El Tribunal Europeo de Derechos Humanos: organización y funcionamiento», en *UNED. Anuario de la Escuela de Práctica Jurídica*, núm. 1, págs. 14. Disponible en Internet: http://www2.uned.es/escuela-practica-juridica/AEPJ%201%20Julia%20Ruiloba.pdf [consulta: 05 de febrero de 2016]; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2011a), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 72. Disponible en Internet: http://fra.europa.eu/en/publication/2011/access-justice-europe-overview-challenges-and-opportunities [consulta: 28 de noviembre de 2015]; Pasquale GIANNITI (a cura di) (2015), *La CEDU e il ruolo delle Corti: globalizzazione e promozione delle libertà fondamentali*, Bologna, Zanichelli, XLVII, págs. 2032.

[151] Muchos gobiernos han aumentado el control de los ciudadanos con el fin de prevenir la delincuencia y el terrorismo. Esto ha significado que la cuestión se llevara ante las máximas autoridades jurisdiccionales europeas, el Tribunal de Justicia de la Unión Europea (*vid*. Capítulo IV) y el TEDH.

[152] Por ejemplo, en este sentido podemos incluir los programas de vigilancia británicos ("*Investigatory Powers Bill*") que violan el Convenio. *Vid*. Matt BURGESS (2016), «UN warns UK's IP Bill 'undermines' the right to privacy», en *wired.com.uk*. Disponible en Internet: http://www.wired.co.uk/article/un-privacy-ip-bill-not-compliant-international-law [consulta: 28 de marzo de 2016].

108. La extensa jurisprudencia del TEDH, que se ha visto en la obligación de pronunciarse en situaciones de crisis de seguridad nacional desde ya hace algunas décadas, es una fuente indispensable para entender correctamente el sentido del artículo 8 del CEDH. El Tribunal ha sostenido sistemáticamente que el almacenamiento y conservación de datos personales por parte de la policía o de las autoridades nacionales de seguridad constituye una injerencia, con arreglo al artículo 8, apartado 1, del CEDH. Pero, también, hay muchas sentencias del TEDH que abordan la justificación de dichas injerencias mediante la vigilancia del Estado.

109. Desde aquí, representamos un breve *excursus*, más o menos cronológico, de la más representativa jurisprudencia del TEDH desde la "clásica" hasta nuestros días −en que se inscribe la presente investigación−, con el fin de evaluar la forma en que ha evolucionado la acción del Tribunal referente a ese conflicto entre la protección de la privacidad y seguridad pública (y consiguiente lucha contra la criminalidad[153]), y la protección de la privacidad de la mano del derecho al respecto de la vida privada, del domicilio y de la correspondencia reconocido en el citado artículo 8 del CEDH.

110. La primera sentencia del Tribunal, en referencia al asunto en cuestión, ha dado lugar, a finales de los años 70, a la inclusión de la protección de las conversaciones telefónicas dentro del artículo 8 del CEDH. Así, en el asunto *Klass y otros contra Alemania*[154], el TEDH no reconoce la violación del artículo 8 del CEDH, porque el segundo apartado del mismo artículo contempla las limitaciones al derecho del individuo al respeto de la vida privada y de su correspondencia, ya sea por escrito o por teléfono. Reconoce que las sociedades democráticas están amenazadas por el terrorismo y que el Estado debe ser capaz, con el fin de contrarrestar de manera eficaz esa amenaza, de llevar a cabo una vigilancia secreta de los «elementos subversivos» que operan en su territorio. En el caso en examen, el control secreto sobre la vida y las comunicaciones de la persona era legítimo y conforme a lo dispuesto por una ley parlamentaria y la Constitución Federal alemana, necesarias para defender la sociedad democrática en Alemania contra la amenaza de espionaje y terrorismo[155].

[153] Sobre la lucha contra la criminalidad y los derechos fundamentales de la UE, *vid*. Silvia RIGHI (2014), *Lotta alla criminalità e salvaguardia dei diritti e delle libertà fondamentali nell'U.E.*, Tesis Doctoral, Bologna, Alma Mater Studiorum - Università di Bologna, Dottorato di Ricerca in Diritto Europeo, Ciclo XXVI, págs. 309.

[154] TEDH, *Klass y otros contra Alemania*, núm. 5029/71, sentencia de 6 de septiembre de 1978. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57510 [consulta: 07 de febrero de 2016].

[155] Alicia GONZÁLEZ MONJE (2017), «Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto», en *Revista Europea de Derechos Fundamentales*, núm. 29, pág. 285. Disponible en Internet: http://journals.sfu.ca/redf/index.php/redf/article/view/224 [consulta: 02 de febrero de 2018]. Sin embargo, el

111. Las principales decisiones del TEDH en casos de protección de datos atañen, inicialmente, al uso de éstos por los poderes públicos. Las decisiones jurídicas se orientaron fundamentalmente a la evaluación de las medidas adoptadas por los Estados, llamados a equilibrar al mismo tiempo la necesidad de proteger la privacidad con la circulación de la información dentro de las administraciones públicas[156].

112. En 1987, por primera vez, una sentencia de la Corte afronta el problema de la recogida, almacenamiento y utilización de datos personales por parte de la autoridad pública (es decir, las fuerzas de inteligencia), como actividad que afecta a la vida privada de una persona. En el caso *Leander contra Suecia*[157], el TEDH resolvió que «*el control secreto de personas que solicitan puestos de importancia para la seguridad nacional no es contrario, en sí mismo, a una sociedad democrática*»[158]. En particular, el Tribunal concluyó que «*las garantías específicas establecidas en la legislación nacional para la protección de los intereses del interesado, por ejemplo, los controles ejercidos por el Parlamento y el Ministro de Justicia, derivaron en que* (…) *el sistema de control de personal de Suecia cumplía los requisitos del artículo 8, apartado 2, del CEDH*»[159]. Verificado el "amplio margen de apreciación disponible", el Estado demandado estaba autorizado a considerar que, en el asunto planteado por el demandante, «*los intereses de la seguridad nacional prevalecían sobre los intereses individuales*». El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH[160].

TEDH añadió una advertencia, reconociendo que la vigilancia y el control de las comunicaciones secretas debe hacerse sólo en circunstancias excepcionales en cuantos tales controles caracterizan un Estado policial y que la ley de emergencia puede atentar e incluso destruir la democracia, cuando por el contrario afirma defenderla.

[156] Consideremos el caso de la conservación de los datos sanitarios en los hospitales y su secreto, el derecho de que los datos de los registros de antecedentes penales no se utilicen para fines distintos de aquellos para los que fueron recogidos, o el derecho al secreto de las comunicaciones telefónicas. Por cuánto concierne la conservación de los datos sanitarios en los hospitales y su secreto, *vid*. TEDH, *Z. contra Finlandia*, núm. 22009/93, sentencia de 25 de febrero de 1997. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-58033#{%22itemid%22:[%22001-58033%22]} [consulta: 06 de junio de 2015]. *Vid*., asimismo, con respecto al tratamiento de los datos personales relacionados el estado de salud, TEDH, *M.S. contra Suecia*, núm. 20837/92, sentencia de 27 de agosto de 1997.

[157] TEDH, *Leander contra Suecia*, núm. 9248/81, sentencia de 26 de marzo de 1987. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57519#{%22itemid%22:[%22001-57519%22]} [consulta: 06 de junio de 2015].

[158] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014), *Manual de legislación europea en materia de la protección de datos*, Luxemburgo, pág. 72. Disponible en Internet: http://www.echr.coe.int/Documents/Handbook_data_protection_SPA.pdf [consulta: 12 de mayo de 2015]. El TEDH ha declarado que «*el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue*». TEDH, *Leander contra Suecia*, apartado 58.

[159] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 72).

[160] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 72). Del mismo modo, en el asunto *B.B. contra Francia*, el TEDH decidió que la inclusión de un delincuente sexual convicto en una base de datos nacional judicial, entraba en el ámbito de aplicación del artículo 8 del CEDH, y, por tanto, no había existido una violación del artículo 8 del CEDH. TEDH*, B.B. contra Francia*, núm. 5335/06,

113. En los años 90 tenemos las primeras sentencias en las que el TEDH cuestionó el alcance expansivo del artículo 8 del CEDH[161], en relación con el concepto de vida privada[162], aunque no se pronunció sobre el tema en concreto de las nuevas tecnologías. Sobre todo, el Tribunal se fijó en el aspecto del derecho a la vida privada y familiar, en relación con las bases de datos como medio de almacenamiento, comunicación y difusión de datos, en términos de protección de la interferencia directa de los poderes públicos.

114. Sobre las actividades investigadoras, llevadas a cabo en secreto por la autoridad judicial, como las interceptaciones de las comunicaciones, que requieren una ley que especifique las condiciones y circunstancias de aplicación, el Tribunal de Estrasburgo se ha pronunciado en la importante sentencia *Malone contra el Reino Unido*[163]. El caso trató una investigación penal sobre dos sujetos, a los que se habían tomado muestras genéticas y huellas dactilares. Posteriormente, las investigaciones concluyeron con la absolución, pero las bases de datos de la policía británica continuaron manteniendo los datos almacenados y la policía misma rechazó la solicitud de destrucción realizada por los interesados. El TEDH subrayó cómo la protección de los datos personales constituye un aspecto esencial del derecho a la vida privada y familiar y al mismo tiempo considera legítimo el objetivo de las autoridades públicas de conservar datos por la finalidad de investigación penal y prevención de los delitos; pero, en esta circunstancia específica, se consideró que el almacenamiento del perfil biológico tan profundo e ilimitado en el tiempo ha sido considerado como desproporcionado. El Tribunal sostuvo que había una violación del artículo 8 del CEDH[164].

---

sentencia de 17 de diciembre de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-96361#{"itemid":["001-96361"]} [consulta: 20 de febrero de 2016].

[161] Esther SALAMANCA AGUADO (2014), «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», en *Revista del Instituto Español de Estudios Estratégicos (IEEE)*, núm. 4, págs. 26. Disponible en: http://revista.ieee.es/index.php/ieee/article/view/137 [consulta: 19 de noviembre de 2015].

[162] TEDH, *Niemietz contra Alemania*, núm. 13710/88, sentencia de 16 de diciembre de 1992. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57887#{"itemid":["001-57887"]} [consulta: 19 de noviembre de 2015]. En particular, en el apartado 29: «*(...) no considera posible o necesario intentar elaborar una definición exhaustiva de la noción de "vida privada". Sin embargo, resultaría en exceso restrictivo limitar esta noción al "círculo íntimo" en el cual la persona vive su vida personal como lo elija, y excluir de él completamente el mundo exterior no contemplado en ese círculo". Sobre la vida privada, ésta también debe incluir en cierto grado el derecho a establecer y desarrollar relaciones con otros seres humanos"»*. Sobre el caso, *vid*. Cristina HERMIDA DEL LLANO (2005), *Los derechos fundamentales en la Unión Europea*, Barcelona, Anthropos Editorial, pág. 74.

[163] TEDH, *Malone contra el Reino Unido*, núm. 8691/79, sentencia de 02 de agosto de 1984. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57533#{%22itemid%22:[%22001-57533%22]} [consulta: 06 de junio de 2015]. También en Esther SALAMANCA AGUADO (2014: 10 y ss.).

[164] Otra de las cuestiones principales es lo que se menciona en el caso *Kopp contra Suiza* al producirse la ilegalidad de investigaciones y escuchas telefónicas del abogado *Kopp*. El TEDH indica que el objeto del artículo 8 «*exige que la ley sea «compatible con la preeminencia del derecho»: cuando se trata de medidas secretas de vigilancia o de interceptación de comunicaciones por las autoridades públicas, la ausencia de control público y el riesgo de abuso de poder implican que el derecho interno debe ofrecer al individuo una*

115. Utilizando la jurisprudencia del TEDH, debería ser posible evaluar el efecto de la interferencia en el individuo, a fin de brindar a la persona una protección adecuada contra acciones arbitrarias del Estado. En su sentencia sobre el caso *Malone*, el Tribunal de Estrasburgo subrayó que el procedimiento debe tener una base jurídica precisa, clara y accesible[165]. Dicha base jurídica debería establecerse en una ley que sea de fácil acceso para el público y que debería explicar la naturaleza de las ofensas que pueden dar lugar a una orden de intercepción o vigilancia. La ley también debe definir las categorías de personas que podrían estar sujetas a vigilancia[166]. Las medidas adoptadas deberían limitarse en lo que respecta a la duración.

116. Por otro lado, el requisito de la necesidad[167], citado en el apartado segundo del artículo 8, implica que la injerencia en el derecho a la intimidad debe corresponder a una necesidad acuciante de la sociedad, y ser pertinente, adecuada y proporcionada a la finalidad legítima que tiene como objetivo proteger. En este sentido se coloca el caso *Amann contra*

cierta protección contra las injerencias arbitrarias en los derechos garantizados por el artículo 8» (apartado 64). Como se expone también en el apartado 72 de la sentencia, «*las escuchas y los demás procedimientos para interceptar las conversaciones telefónicas, representan una ofensa grave al respeto de la vida privada y de la correspondencia*» como sucedió en las vulneraciones cometidas por la *NSA* y las agencias europeas al espiar a ciudadanos europeos. TEDH, *Kopp contra Suiza*, núm. 23224/1994, sentencia de 25 de marzo de 1998. Disponible en Internet: http://lawcenter.es/w/file/download/66097 [consulta: 08 de junio de 2015]. Otra sentencia del TEDH en que declara una violación del artículo 8 del CEDH, por injerencia en el derecho a la protección de datos mediante la vigilancia, se encuentra en el asunto *Allan contra el Reino Unido*. TEDH, *Allan contra el Reino Unido*, núm. 48539/99, sentencia de 5 de noviembre de 2002. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-60713#{"itemid":["001-60713"]} [consulta: 02 de octubre de 2016].

[165] TEDH, *Malone contra el Reino Unido*, apartado 67: «*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8* (…). *The subsequent use of the stored information has no bearing on that finding* (…). *However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained* (…)».

[166] Por último, recordando el juicio en Weber y Saravia, se reafirma que el procedimiento a seguir para examinar, utilizar y almacenar los datos obtenidos, las precauciones que deben tomarse al comunicar los datos a otras partes y las circunstancias en las que los materiales que resultaron de tal interferencia pueden o deben ser destruidos, debe ser previsible también. Está claro que los riesgos de arbitrariedad son especialmente evidentes cuando una facultad conferida al ejecutivo se ejerce en secreto. La ley debe incluir lo suficientemente claro términos para dar a los ciudadanos una indicación adecuada sobre las circunstancias y las condiciones según las cuales las autoridades públicas están facultadas para recurrir a tales medidas. TEDH, *Weber y Saravia contra Alemania*, núm. 54934/00, sentencia de 29 junio 2006, apartado 95. Disponible en Internet: https://hudoc.echr.coe.int/eng#{"itemid":["001-76586"]}[consulta: 02 de octubre de 2016]. *Amplius*, *vid*. Alicia GONZÁLEZ MONJE (2017: 286-287).

[167] TEDH, *Kruslin contra Francia*, núm. 11801/85, sentencia de 23 de abril de 1990. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"fulltext":["Kruslin"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57626"]} [consulta: 10 de marzo de 2016]; TEDH, *Valenzuela Contreras contra España*, núm. 58/1997/842/1048, sentencia de 30 de junio de 1998. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"fulltext":["Valenzuela"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-58208"]} [consulta: 11 de marzo de 2016]. Esther SALAMANCA AGUADO (2014: 10-12).

Suiza[168], donde las autoridades interceptaron una llamada telefónica de negocios del demandante. Sobre esta llamada, las autoridades investigaron al demandante y abrieron una ficha sobre él en el fichero de seguridad nacional[169]. No obstante la interceptación afectaba a una llamada telefónica de negocios, el TEDH consideró que «*el almacenamiento de datos sobre dicha llamada estaba relacionado con la vida privada del demandante*»[170]. El Tribunal señaló que «*el término vida privada no debía interpretarse de forma restrictiva, en particular, teniendo en cuenta que el respeto a la vida privada incluye el derecho a entablar y desarrollar relaciones con otros seres humanos*»[171]. Asimismo, «*no existía una razón de principio que justificara la exclusión de las actividades de carácter profesional o de negocios del concepto de "vida privada"*»[172]. Además la injerencia en el caso del demandante no había sido realizada de conformidad con la ley dado que el derecho nacional «*no incluía disposiciones específicas y detalladas sobre la obtención, el registro y el almacenamiento de información*»[173]. El TEDH concluyó que existía una violación del artículo 8 del CEDH.

117. El Tribunal reconoce que el mero hecho de conservar los datos personales de un individuo constituye una injerencia en la vida privada de este último. También constituye una violación la denegación de acceso a las informaciones recogidas y presentación de la solicitud de cancelación. El Tribunal da un significado absoluto a esta interferencia: no importa si los datos son sensibles o no. Tampoco es esencial saber si las autoridades públicas han usado esta información personal o no. Ya la obtención y almacenamiento que se hacen

[168] TEDH, *Amann contra Suiza* [GS], núm. 27798/95, sentencia de 16 de febrero de 2000. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-58497#{%22itemid%22:[%22001-58497%22]} [consulta: 06 de junio de 2015].

[169] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 39).

[170] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 40).

[171] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 40). *Cfr*. TEDH, *Rotaru contra Romania* [GS], núm. 28341/95, sentencia de 04 de mayo de 2000. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"appno":["28341/95"],"itemid":["001-58586"]} [consulta: 15 de marzo de 2016]. El concepto de "vida privada", incluye varios tipos de información personal, como: los estudios conseguidos; la realización de actividad política; las condenas penales. No hacen hincapié en el hecho de que dichas informaciones se refieran al pasado, ya sea de dominio público o confidencial. Esther SALAMANCA AGUADO (2014: 17).

[172] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 40). Esta interpretación amplia, esta vez ligado al nuevo elemento tecnológico de los procesadores de datos y la protección necesaria, basándose en un parámetro externo a la CEDH, vale a decir sobre el Convenio n. 108 (*vid*. *infra*). TEDH, *Amann contra Suiza*, núm. 27798/95, apartado 65: «*That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)*».

[173] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 40).

constituyen una interferencia del Estado en la esfera privada de la persona. La conservación de las noticias sobre la vida privada de una persona en un registro secreto y su comunicación, por tanto, entra dentro del ámbito del artículo 8, apartado 1, del CEDH. La misma norma también prevé excepciones al principio de respeto a la vida privada, la cual sin embargo debe interpretarse en sentido estricto.

118. Aunque el TEDH reconoce la legitimidad de los servicios de inteligencia en una sociedad democrática, reitera que en virtud del CEDH el poder de vigilancia secreta con respecto de los ciudadanos será posible si se encuentra prescrito por la ley y en la medida estrictamente necesaria para salvaguardar instituciones democráticas[174]. Cuando los datos personales se recopilan sin el conocimiento del interesado, éste deberá ser informado de la recogida de los datos tan pronto como dicha divulgación no represente un obstáculo para las investigaciones. La recopilación de datos mediante vigilancia técnica u otros medios automatizados también debería estar basada en disposiciones legales específicas[175].

119. Después los años 2000, sobre todo, el Tribunal ha ampliado la noción de "vida privada y familiar" contenida en el artículo 8 del CEDH, incluyendo una gama muy amplia de situaciones jurídicas[176]. Pero esta vez, añadiendo también el elemento tecnológico de los procesadores de datos y la protección necesaria que va con ella, basándose en un parámetro externo del CEDH y tomando como fuente de inspiración el Convenio del Consejo de Europa n. 108 sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Esto sucede, por ejemplo, en los asuntos *Z. contra Finlandia* y *Amann contra Suiza*. Por lo tanto, los jueces han entendido el alcance del artículo 8 del

[174] La ley deberá ser «*accesible para las personas a las cuales concierna y previsible en cuanto a sus efectos*». TEDH, *Amann contra Suiza*, apartado 50. Una norma es previsible «*si está formulada con la suficiente precisión como para permitir que cualquier persona* (…) *regule su comportamiento*» (apartado 56). AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 69-70). Lo mismo en el asunto *Rotaru contra Rumanía*, el TEDH consideró «*que existía una violación del artículo 8 del CEDH porque la legislación rumana permitía la recopilación, el registro y el almacenamiento en archivos secretos de información que afecta a la seguridad nacional, sin establecer límites en el ejercicio de dichos poderes, los cuales quedaban a discreción de las autoridades*». En definitiva, la legislación nacional no cumplía el requisito de previsibilidad según el artículo 8 del CEDH y que se había violado dicho artículo. Especialmente en relación con los requisitos de prevención y detección de los delitos, así como la seguridad, véanse además TEDH, *Taylor-Sabori contra el Reino Unido*, núm. 47114/99, de 22 de octubre de 2002. *Vid*. AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 70).

[175] *Vid*. TEDH, *Vetter contra Francia*, núm. 59842/00, sentencia de 31 de mayo de 2005. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-69188#{"itemid":["001-69188"]} [consulta: 15 de junio de 2016].

[176] Esther SALAMANCA AGUADO (2014: 9 y ss.). En esta gama se incluye: la pretensión de no ser espiado reconocido y controlado de forma remota, la de que puede controlar la cantidad y la calidad de sus datos que otros detengan, al derecho a ver protegida su salud y seguridad personal, de adoptar niños sin discriminación y de formar una familia y elegir el apellido.

CEDH a la protección de los datos personales y el poder de control de la circulación de la información personal, explícitamente referidos en el Convenio n. 108 (*vid*. *infra*).

120. La jurisprudencia ha aclarado que existe una estrecha relación entre los dos textos, y señaló que la protección de los datos personales representa una aplicación específica del derecho a la privacidad. De esta manera se ha ampliado la argumentación incorporando dentro del artículo 8 del CEDH la protección de los datos personales, una interpretación en la que se hizo referencia al nuevo elemento tecnológico por los datos procesados por Internet. Por consiguiente, cae dentro de la protección del artículo 8 del CEDH cualquier restricción del derecho a la privacidad que se produzca en relación con el tratamiento de datos personales mediante el uso de técnicas de investigación o de control invasivo de la esfera íntima.

121. Respecto al aspecto del derecho a la vida privada y familiar, en relación con las bases de datos y los usos de Internet[177] como medio de conservación, comunicación y difusión de datos[178], el caso más importante entre los recientes (con respecto a la interferencia directa de las públicas potestades) es el caso *S. and Marper contra Reino Unido*. En este asunto, de hecho, la Corte ha aplicado directamente el juicio de proporcionalidad en el que la conservación de los datos biométricos fue proporcionada por la ley británica, averiguando la relación entre la idoneidad de los efectos de una medida y los medios utilizados para su

[177] En 2007, de hecho, la Web hizo su entrada formal en virtud, como dicho, de la extensión del artículo 8 del CEDH. En este sentido, entre los casos más emblemáticos y conocidos nos parece el caso *Copland contra el Reino Unido*. El caso contempló el uso del teléfono, el correo electrónico y de Internet por una empleada de una universidad, objeto de vigilancia de forma secreta, a fin de averiguar si estaba haciendo un uso excesivo de los servicios de dicha institución con fines personales. El TEDH sostuvo que las llamadas telefónicas desde las instalaciones profesionales quedan amparadas por los conceptos de vida privada y correspondencia. Por tanto, las llamadas y los correos electrónicos enviados desde el trabajo, así como la información que deriva del control del uso personal de Internet, quedaban protegida por el artículo 8 del CEDH. En el caso de la demandante, no existían disposiciones que regulasen las circunstancias en que los empresarios podrían controlar el uso del teléfono, el correo electrónico y de Internet por parte de los empleados. Por tanto, la injerencia no se había producido de conformidad con la ley. El Tribunal concluyó que había violación del artículo 8 del CEDH. TEDH, *Copland contra el Reino Unido*, núm. 62617/00, sentencia de 3 de julio de 2007. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-79996#{%22itemid%22:[%22001-79996%22]} [consulta: 06 de junio de 2015]. Apartado 41: «*According to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8 § 1* (…). *It follows logically that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage*». Ofelia TEJERINA RODRÍGUEZ (2014), *Seguridad del Estado y privacidad*, Madrid, Editorial Reus, pág. 222.

[178] El potencial de Internet, lo que reduce las distancias y las fronteras y permite al usuario conectarse con la gente y los archivos relacionados con la misma en cualquier parte del mundo, destaca sin embargo una serie de problemas de la protección social y jurídica, incluida la de los datos personales. En ese contexto, *vid*. Pablo Lucas MURILLO DE LA CUEVA y José Luis PIÑAR MAÑAS (2009), *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, págs. 184.

consecución, como control del margen nacional de apreciación[179]. Durante una investigación penal en contra de dos personas, a las que se les han tomado muestras y huellas genéticas. Posteriormente, las investigaciones concluyeron de modo absolutorio, pero la base de datos de la policía británica continuó manteniendo los datos almacenados y lo mismo policía rechazó la solicitud de destrucción formulada por los interesados. El Tribunal dictaminó que, como resultado de una absolución en un caso criminal, constituyen una injerencia ilegal en su vida privada el rechazo de la autoridad estatal a borrar los datos personales relativos a las huellas dactilares del solicitante, perfiles de ADN y muestras celulares. Se trata, de hecho, de datos personales que conciernen a personas identificadas o identificables. La expansión del uso de las bases de datos de ADN debe respetar los límites del equilibrio con el interés, en competencia, de la protección de la intimidad. El desarrollo de nuevas tecnologías implica una responsabilidad especial de los Estados contrayentes para identificar el correcto equilibrio de intereses. La legislación nacional deberá prever las medidas adecuadas para evitar cualquier uso no conforme con la protección de los derechos garantizados por el artículo 8 del CEDH[180]. La Corte concluye que el carácter general e indiscriminado del mecanismo de conservación de huellas dactilares, de las muestras celulares y perfiles de ADN de personas sospechosas de la comisión de ciertos delitos, pero no condenados, no garantiza un «*justo equilibrio*» de «*los intereses públicos y privados en juego*»[181]. El TEDH ha subrayado cómo la protección de los datos personales constituye un aspecto esencial del derecho a la vida privada y familiar y al mismo tiempo ha creído objetivo legítimo de las autoridades públicas mantener los datos con fines de investigación penal y prevención del delito; pero, en esta circunstancia específica, se trató de sujetos cuyas posiciones fueron archivadas por lo que el perfil biológico de modo profundo y temporalmente ilimitado se consideró desproporcionada[182]. El Tribunal de Estrasburgo confirma que había existido una injerencia en el derecho protegido por del artículo 8 del CEDH.

122. Conforme con el aspecto del derecho a la vida privada y familiar, pero también en relación con la insuficiente protección ofrecida por las autoridades al derecho mismo, parece

[179] TEDH, *S. and Marper contra Reino Unido*, núm. 30562/04 y núm. 30566/04, sentencia de 4 de diciembre de 2008. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-90051#{%22itemid%22:[%22001-90051%22]} [consulta: 10 de junio de 2015]; Gloria GONZÁLEZ FUSTER (2009), «TEDH - Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas», en *Revista de Derecho Comunitario Europeo*, núm. 33, págs. 619-633. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=679&IDA=27523 [consulta: 11 de noviembre de 2015].

[180] Se remite a la sentencia TEDH, *Leander contra Suecia*, núm. 9248/81, de 26 de marzo de 1987.

[181] Gloria GONZÁLEZ FUSTER (2009: 630).

[182] Gloria GONZÁLEZ FUSTER (2009: 630-631); Beatriz S. TOMÁS MALLÉN (2014: 226).

el destacado caso *K.U. contra Finlandia*[183]. Se detectó la violación del artículo 8 del país escandinavo, debido a la insuficiente protección garantizada a un menor de edad por la legislación, cuyos datos personales habían sido publicados "*online*" en un sitio de citas. El demandante solicitó a los tribunales nacionales que ordenara al proveedor de servicios de Internet proporcionar la identidad de la persona física a la que se atribuyó la dirección *IP* utilizada para la conexión y publicación del anuncio, pero sin éxito[184]. El TEDH resolvió que los Estados no solo estaban obligados a abstenerse de realizar injerencias arbitrarias en las vidas privadas de las personas físicas sino que, también, pueden quedar sometidos a obligaciones positivas que impliquen «*la adopción de medidas destinadas a garantizar el respeto a la vida privada, incluso en el ámbito de las relaciones entre las personas físicas*»[185]. En el caso del demandante, su protección práctica y efectiva exigía que se adoptaran medidas eficaces para identificar y enjuiciar al autor. Sin embargo, el Estado no proporcionaba dicha protección y el TEDH pronunció que había violación del artículo 8 del CEDH[186]. En este juicio, con el concepto de obligaciones positivas, el Tribunal de Estrasburgo logra establecer la responsabilidad de los particulares, a saber, los operadores de redes[187].

123. En una serie de decisiones recientes, el Tribunal de Estrasburgo ha establecido la violación del Convenio por la legislación antiterrorista adoptada por algunos Estados

[183] TEDH, *K.U. contra Finlandia*, núm. 2872/02, sentencia de 2 de marzo de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-89964#{%22itemid%22:[%22001-89964%22]} [consulta: 10 de junio de 2015].

[184] En particular, ni el Tribunal de primera instancia ni el de Apelación acogieron la solicitud, basándose en la ausencia de una predicción que, en relación a los delitos asumidos en este caso, autorizara la divulgación de los datos personales por parte del proveedor. Una obligación en tal sentido, de hecho, de acuerdo con la legislación finlandesa, existía sólo en la presencia de ciertos delitos.

[185] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 135). *Vid*. TEDH, *K.U. contra Finlandia*, apartado 43: «*These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue*».

[186] TEDH, *K.U. contra Finlandia*, apartado 49: «(…) *Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged* (…)».

[187] Esta sentencia, por primera vez, involucra a los operadores de redes, que son entidades privadas, aunque cada vez más titulares de funciones públicas de interés (*Internet Service Providers - ISP*). Según el Tribunal, una protección práctica y efectiva del demandante, en nombre de la cual, y sin su conocimiento se había publicado ilegalmente un anuncio en Internet implicaba la adopción de medidas eficaces para identificar y procesar al autor del anuncio. En este último caso, de hecho, el comportamiento asumió la naturaleza criminal.

contratantes, que contiene un endurecimiento injustificado de los poderes de investigación de las autoridades nacionales contra los sospechosos de aquellos delitos asociados al terrorismo internacional, sobre la base de las disposiciones de la legislación de Estados Unidos después del 11 de septiembre.

124. Recordamos el caso *Gillan y Quinton contra Reino Unido*[188], en el que el TEDH falló contra el Reino Unido por incumplimiento del artículo 8 del Convenio, debido a una considerable restricción de las libertades personales de acuerdo con el *Terrorism Act 2000*. En particular, el Tribunal examinó el amplio margen de discrecionalidad conferido por la ley, en términos de autorización del poder de detener y registrar y su aplicación en la práctica, y que no ha sido cubierto por garantías legales adecuadas que permitan una protección individual adecuada frente a una injerencia arbitraria[189].

125. Se debe enfatizar, sin embargo, que el Tribunal no siempre ha condenado a los Estados por violación del artículo 8. En este sentido, recordamos el asunto *Gardel contra Francia*[190], a los objetivos de la inscripción de los autores de delitos sexuales en un expediente judicial nacional, en el que la Corte afirmó la excepción de la protección de los datos personales por razones de seguridad. El asunto trata el caso de un hombre con condena en firme por asalto sexual contra un menor. El nombre del acusado había sido inscrito en el registro requerido por la ley francesa de los individuos peligrosos en relación a los delitos sexuales ("*sex offenders*")[191]. El TEDH consideró que la legislación francesa prevé un límite de tiempo (20 y 30 años, dependiendo del caso) y que en todo caso se trató definitivamente de un sujeto condenado y, por lo tanto, que no hay violación. En conclusión, el Tribunal declara que el registro de los recurrentes en las bases de datos constituye un equilibrio de los intereses públicos y privados en juego y que el Estado demandado no ha excedido el margen de apreciación nacional[192].

---

[188] TEDH, *Gillan y Quinton contra Reino Unido*, núm. 4158/05, sentencia de 12 enero 2010. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-139040#{"itemid":["001-139040"]} [consulta: 31 de octubre de 2016].

[189] En Omar BOUAZZA ARIÑO (2010), «Notas de jurisprudencia del Tribunal Europeo de Derechos Humanos», en *Revista de Administración Pública*, núm. 183, Madrid, pág. 274. ISSN: 0034-7639; Beatriz S. TOMÁS MALLÉN (2014: 224).

[190] TEDH, *Gardel contra Francia*, núm. 16428/05, sentencia de 17 de marzo de 2010. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-96457#{"itemid":["001-96457"]} [consulta: 10 de junio de 2015].

[191] David HARRIS, Michael O'BOYLE, Edward BATES, and Carla BUCKLEY (2014: 499).

[192] En el mismo filón del caso *Gardel*, son otras dos acciones contra Francia que se decidieron en 2009, *Bouchacourt contra Francia* y *M.B. contra Francia*. En las sentencias el TEDH ha reafirmado el papel fundamental de la protección de los datos personales objeto de tratamiento automático, especialmente por razones de seguridad, sin embargo, llegó a la conclusión de que la inscripción de los recurrentes en un fichero automatizado jurídico nacional para los autores de delitos sexuales no era contraria al artículo 8 del CEDH.

126. En la misma línea, en el asunto *Öcalan contra Turquía* (n. 2)[193], el Tribunal finalizó que no hubo violación del artículo 8 del CEDH con respecto al fundador de la organización considerada ilegal "Partido de los Trabajadores del Kurdistán" (PKK), tras entender que el temor legítimo del gobierno turco sobre la posible utilización de las comunicaciones con el exterior para contactar con miembros del PKK habilitaba a las autoridades turcas para proceder a esa restricción del respeto a su privacidad −se denunciaban los obstáculos a sus comunicaciones telefónicas, a su correspondencia y a las visitas de los miembros de su familia y de sus abogados− al no exceder de lo necesario para la defensa del orden público y la prevención de las infracciones penales[194].

127. Desde otra perspectiva, el TEDH ha sostenido que la disciplina interna que limita la posibilidad, para los individuos, de tener acceso directo, y para hacer rectificaciones, a los datos personales contenidos en la base de datos del Sistema de Información Schengen, no da lugar a violación de artículos 6 y 8 del Convenio.

128. En el caso *Dalea contra Francia*, un ciudadano rumano al cual se denegó el visado para viajar a Alemania y, luego, un visado para viajar a Francia, al estar señalado por las autoridades francesas en la base de datos del Sistema de Información Schengen, tuvo como efecto su no admisión. El recurrente lamentó la violación de los principios de "juicio justo" (artículo 6, apartado 1 - Derecho a un proceso equitativo) y de la protección de la vida privada (artículo 8), tomando nota de no haber obtenido comunicaciones de las informaciones que le conciernen contenidas en la base de datos de la sección nacional francesa del Sistema de Información Schengen y su corrección o eliminación[195]. El TEDH ha explicado su decisión, teniendo en cuenta, en primer lugar, que el derecho convencional

Nicole ATWILL (2010), «European Court of Human Rights; France: Registration in French National Sex Offender Database Does Not Violate Rights», en *The Library of Congress*, Washington. Disponible en Internet: http://www.loc.gov/law/foreign-news/article/european-court-of-human-rights-france-registration-in-french-national-sex-offender-database-does-not-violate-rights/ [consulta: 12 de junio de 2015].

[193] TEDH, *Abdullah Öcalan contra Turquía*, números 24069/03, 197/04, 6201/06 y 10464/07, sentencia de 18 de marzo de 2014. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-142086#{"itemid":["001-142086"]} [consulta: 15 de junio de 2015].

[194] Beatriz S. TOMÁS MALLÉN (2014: 224).

[195] TEDH, *Dalea contra Francia*, núm. 964/07, sentencia de 2 de febrero de 2010. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["863599"],"itemid":["001-97520"]} [consulta: 15 de junio de 2015]. El TEDH rechazó el recurso, teniendo en cuenta, en primer lugar, que el procedimiento establecido por la legislación francesa para permitir a las personas interesadas acceder a sus datos personales en la base de datos de Schengen y, si fuera necesario, hacer que se modifiquen o supriman, es estrechamente relacionada con la disciplina relativa a la entrada y residencia de los extranjeros, en particular con los procedimientos de expedición de visados. En este sentido, la Corte sostuvo que las decisiones relativas a la entrada, residencia y expulsión de extranjeros no dan lugar a disputas sobre los derechos y obligaciones civiles ni están relacionados con los fundamentos de la acusación penal, en el sentido del artículo 6, apartado 1, del CEDH, y por lo tanto no entran dentro del alcance de esta disposición.

no sanciona como tal cualquier derecho de entrada y residencia en un Estado del que sea nacional; asimismo, señala que la injerencia en la vida privada de la persona afectada, debido a la inscripción en la base de datos de Schengen por las autoridades francesas, estaba prevista por la ley y perseguía el objetivo legítimo de proteger la seguridad nacional.

129. Por el hecho de figurar en una lista[196], en el juicio final de la Gran Sala, en la controversia *Nada contra Suiza*[197], el TEDH dictaminó por unanimidad que se había producido violación del artículo 8; y violación del mismo artículo en combinación con el artículo 13 del CEDH (Derecho a un recurso efectivo)[198]. La controversia se refiere a la interdicción del recurrente a la libre circulación, además de la inclusión de su nombre en una lista anexa a la Ordenanza federal suiza sobre los talibanes, adoptada en aplicación de resoluciones del Consejo de Seguridad de las Naciones Unidas en el marco de la lucha contra el terrorismo[199]. Con base en el artículo 8 del CEDH, el Tribunal reiteró el principio de no interferencia de un Estado en el derecho de toda persona al respeto de su vida privada y familiar, excepto si tal injerencia sea prevista por la ley o constituya una medida necesaria

[196] En este sentido, la sentencia *Shimovolos contra Rusia* considera el registro del solicitante como activista en favor de los derechos humanos en una "*black list*" de la policía. De hecho, durante una cumbre Rusia-Unión Europea, las autoridades rusas habían recibido informaciones acerca de la llegada del solicitante en el lugar de la cumbre ya que su nombre apareció en una base de datos que contenía informaciones sobre la vigilancia de las personas clasificadas como "potenciales extremistas", y procedieron a su detención preventiva. El Tribunal sostuvo que se había violado el artículo 8 del CEDH. Observó en particular que la creación y el mantenimiento de la base de datos y el procedimiento para su funcionamiento se regían por una orden ministerial que nunca se había publicado ni se había hecho accesible al público en general. En consecuencia, el Tribunal concluyó que el derecho interno no indicó suficientemente claro el alcance y la forma de ejercer la facultad discrecional concedida a las autoridades nacionales para recopilar y almacenar información sobre la vida privada de las personas en la base de datos. En particular, no estableció en una forma accesible al público ninguna indicación de las salvaguardias mínimas contra el abuso. El CEDH reafirma los principios fundamentales que guían la legislación de los Estados en esta área (cognoscible, previsible y proceso legislativo de forma democrática). TEDH, *Shimovolos contra Rusia*, núm. 30194/09, sentencia de 21 de junio de 2011. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["886752"],"itemid":["001-105217"]} [consulta: 15 de junio de 2015]. Stefano RUGGERI (2012), *Liberty and Security in Europe: a comparative analysis of pre-trial precautionary measures in criminal proceedings*, Göttingen, V&R Unipress, págs. 21 y ss; Wojciech R. WIEWIÓROWSKI (2017), «Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy», en Gert VERMEULEN, Eva LIEVENS (Eds.), *Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data*, Antwerp-Apeldoorn-Portland, Maklu, pág. 175; Alicia GONZÁLEZ MONJE (2017: 288).

[197] TEDH, *Nada contra Suiza*, núm. 10593/08, sentencia de 12 de septiembre de 2012. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-113121#{"itemid":["001-113121"]} [consulta: 18 de junio de 2015].

[198] Beatriz S. TOMÁS MALLÉN (2014: 225).

[199] En contra del recurrente, Youssef Nada, de nacionalidad italiana y egipcia, residente en *Campione d'Italia* desde 1970, se inició una investigación por el Fiscal General de la Confederación Suiza en 2001, sobre la base de la Resolución 1333 del Consejo de Seguridad de Naciones Unidas. Esta Resolución, sucesivamente integrada en el 2002, repartió un régimen de sanciones en contra de una lista de personas y organizaciones, que sustentaban las relaciones con la red terrorista de *Al-Qaeda* y *Osama Bin Laden* ("Ordenanza sobre los talibanes"). En los años, el Sr. Nada ha solicitado más veces la eliminación de su nombre de la Ordenanza y de la investigación suiza, consiguiendo resultados sólo parciales.

para la seguridad nacional[200]. La complejidad de la controversia se ha incrementado por la posición geográfica de *Campione d'Italia*, de hecho, enclave italiano en territorio suizo. El Tribunal sostuvo que las autoridades suizas no han tenido suficientemente en cuenta la naturaleza específica de la controversia, la duración de las medidas impuestas (prohibición de salir durante al menos 6 años), la nacionalidad, la edad y las condiciones de salud del interesado. El Tribunal también señaló que el Sr. Nada no ha podido solicitar concretamente la cancelación de su nombre en los registros de las jurisdicciones nacionales: por lo tanto, se estableció una violación del artículo 13, que establece el "derecho a un recurso efectivo" ante una instancia nacional[201]. El carácter vinculante de las resoluciones del Consejo de Seguridad de las Naciones Unidas, en cuanto a la lucha contra el terrorismo, no exime a los Estados miembros del CEDH de actuar de manera adecuada con el fin de llegar a una armonización de sus obligaciones internacionales en virtud de las resoluciones del Consejo de Seguridad y aquellas descendientes del CEDH[202].

130. En fin, dos recientes sentencias del TEDH ya nos parecen proporcionar todos los elementos para una evaluación[203] del ejercicio de las autoridades públicas que, sin embargo, no pueden efectuar una obtención indiscriminada y sin control del uso de "grandes datos". Se trata de los juicios *Zakharov contra Rusia*[204], de diciembre de 2015, y sobre todo *Szabó y Vissy contra Hungría*[205], de enero de 2016, en la que el TEDH establece que los dos gobiernos han violado el derecho al respeto de la vida privada y la correspondencia, como exige el artículo 8 del Convenio.

131. En el caso *Roman Zakharov contra Rusia*, el solicitante inició un procedimiento judicial contra tres operadores de redes móviles. Argumentó que se había violado su derecho

[200] Verena PUSATERI (2013), «La Corte EDU su contrasto al terrorismo internazionale e rispetto dei diritti fondamentali. Nota a Corte EDU, sent. 12 settembre 2012, ric. n. 10593/08, Nada c. Svizzera», en *Diritto Penale Contemporaneo*. Disponible en Internet: http://www.penalecontemporaneo.it/d/1935-la-corte-edu-su-contrasto-al-terrorismo-internazionale-e-rispetto-dei-diritti-fondamentali [consulta: 18 de junio de 2015].
[201] Artículo 13 (Derecho a un recurso efectivo) del CEDH: «*Toda persona cuyos derechos y libertades reconocidos en el presente Convenio hayan sido violados tiene derecho a la concesión de un recurso efectivo ante una instancia nacional, incluso cuando la violación haya sido cometida por personas que actúen en el ejercicio de sus funciones oficiales*».
[202] Verena PUSATERI (2013). El TJUE ha llegado a una solución similar en el famoso "caso Kadi" (TJUE, Gran Sala, de 3 de septiembre de 2008 asuntos acumulados C-402/05 P y C-415/05 P), *vid*. Capítulo IV.
[203] *Vid*. *amplius* Alicia GONZÁLEZ MONJE (2017: 288 y ss.).
[204] TEDH, *Roman Zakharov contra Rusia*, núm. 47143/06, sentencia de 4 de diciembre de 2015. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-159324#{"itemid":["001-159324"]} [consulta: 20 de diciembre de 2015].
[205] TEDH, *Szabó and Vissy contra Hungría*, núm. 37138/14, sentencia de 12 de enero de 2016. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-160020#{"itemid":["001-160020"]} [consulta: 20 de diciembre de 2015].

a la privacidad de sus comunicaciones telefónicas, ya que los operadores habían instalado equipos que le permitían al Servicio Federal de Seguridad interceptar sus comunicaciones telefónicas sin autorización judicial previa[206]. Aunque el Sr. Zakharov fue incapaz de demostrar que sus llamadas habían sido interceptadas, el TEDH consideró que los procedimientos operativos que regían la intervención de llamadas telefónicas violaban el artículo 8 del CEDH. El Tribunal sostuvo que las normas internas que rigen la interceptación de comunicaciones no ofrecían garantías adecuadas y efectivas contra la arbitrariedad y el riesgo de abuso. El Tribunal declaró que el Estado ruso había violado el artículo 8 del CEDH en relación con el marco legal que regulaba las medidas de vigilancia secreta de las comunicaciones, y, en concreto, las garantías necesarias que debían regir dichas medidas. En particular, la legislación nacional no exige eliminar los datos almacenados una vez que se ha logrado el objetivo de almacenamiento. Además, aunque se requería autorización judicial, el escrutinio judicial era limitado.

132. Es cierto que la interferencia de los derechos a la privacidad y protección de datos se encuentra con un objetivo de interés general, es decir contribuir a la lucha contra el terrorismo y la delincuencia grave, y luego a la seguridad pública, pero hace falta evaluar rigurosamente el requisito de proporcionalidad. En el caso *Szabó y Vissy*, el Tribunal sostuvo que había habido una violación del artículo 8 del CEDH. Aceptó que era una consecuencia natural de las formas adoptadas por el terrorismo actual que los gobiernos recurrieran a la supervisión masiva de las comunicaciones, para prevenir incidentes inminentes. Sin embargo, el Tribunal no estaba convencido de que la legislación húngara en cuestión proporcionara salvaguardias suficientes para evitar abusos[207]. El alcance de las medidas podría incluir virtualmente a cualquier persona en Hungría, y con las nuevas tecnologías, el gobierno podría interceptar fácilmente masas de datos referentes incluso a personas fuera del rango original de operación. Además, el ordenamiento de tales medidas se realizaba

[206] Roman Zakharov, director del centro regional de San Petersburgo para la Fundación de Defensa de la Glasnost, sospechó que sus llamadas por teléfono móvil estaban siendo interceptadas y presentó una demanda contra el gobierno ruso en el TEDH. *Vid*. INCLO International Network of Civil Liberties Organizations, *Vigilancia y democracia*, págs. 35-37. Disponible en Internet: https://www.inclo.net/pdf/surveillance-and-democracy-sp.pdf [consulta: 19 de septiembre de 2018].

[207] En concreto, la ley antiterrorista húngara llevada a la práctica permitía una actividad de vigilancia indiscriminada, deliberada por decisión del Ministerio de Justicia, sin que sea necesario presentar pruebas capaces de comprobar de ello la necesidad. Todo esto fue acompañado por un periodo esencialmente ilimitado de medidas de control, en ausencia de cualquier forma de supervisión judicial para evitar abusos. *Vid*. Juan Diego SALON PIEDRA (2017), «La intimidad como parte de la dignidad del ser humano en el Convenio europeo de derechos humanos y la Convención americana de derechos humanos», en Juan José LÓPEZ ORTEGA (dir.), *El Derecho a la intimidad: nuevos y viejos debates*, Madrid, Dykinson, pág. 126. Disponible en Internet: http://e-archivo.uc3m.es/bitstream/handle/10016/24016/derecho_intimidad_2017.pdf [consulta: 25 de mayo de 2017].

enteramente dentro del ámbito del ejecutivo y sin una evaluación sobre si la interceptación de las comunicaciones era estrictamente necesaria y si no existían medidas correctivas efectivas, y menos aún judiciales.

133. En las sentencias en cuestión, que se refieren a las medidas de vigilancia e interceptación, el TEDH considera que la conservación de datos con el fin de ponerlos a disposición con fines de investigación en un momento subsiguiente constituye una interferencia con los derechos fundamentales, en particular con el derecho al respeto de la vida privada y la protección de los datos personales de conformidad con el artículo 8 del CEDH. Incluso el acceso de las autoridades nacionales a los datos de los individuos constituye una interferencia con los derechos fundamentales. Esta interferencia es especialmente grave cuando los datos se almacenan y posteriormente se utilizan sin que el usuario sea conocedor de haber sido registrado. Esta circunstancia crea en el individuo la sensación de que su vida privada sea objeto de una vigilancia constante[208].

134. El Tribunal recordó y explicó que la referencia a la "previsibilidad" en el contexto de la interceptación de comunicaciones no puede ser la misma que en muchos otros campos. La previsibilidad en el contexto especial de las medidas secretas de vigilancia, como la interceptación de comunicaciones, no puede significar que un individuo pueda prever cuándo es probable que las autoridades intercepten sus comunicaciones para que pueda adaptar su conducta en consecuencia. La legislación de los Estados miembros debe ser lo suficientemente clara como para dar a los ciudadanos una indicación adecuada sobre cuándo y cómo las autoridades públicas pueden recurrir a medidas de vigilancia[209].

135. Por lo tanto, el TEDH considera que la interferencia en los derechos fundamentales de los ciudadanos sólo puede justificarse si está expresamente prevista por la ley, persigue los objetivos legítimos conforme a lo dispuesto en el artículo 8 del CEDH, y es necesaria en una sociedad democrática para alcanzar dichos objetivos legítimos[210]. Es decir que no sólo que sea necesaria para la preservación de las instituciones democráticas, sino que -en el fallo

[208] NEDERLANDS JURISTEN COMITÉ VOOR DE MENSENRECHTEN (2016), «La ley de escuchas telefónicas rusa es un "queso suizo" judicial, sentencia el Tribunal de Estrasburgo», en *Civil Liberties Union for Europe*, febrero 26. Disponible en Internet: http://www.liberties.eu/es/news/cedh-ve-ley-escuchas-telefonicas-rusas-como-un-queso-suizo-judicial [consulta: 05 de marzo de 2016].
[209] Wojciech R. WIEWIÓROWSKI (2017: 174).
[210] Pilar Eirene DE PRADA (2015), «Privacidad en la era digital: El caso Zakharov», en *Rights International Spain*. Disponible en Internet: http://www.rightsinternationalspain.org/es/blog/92/privacidad-en-la-era-digital:-el-caso-zakharov [consulta: 05 de marzo de 2016].

Szabó y *Vissy* se subraya un requisito totalmente nuevo- la medida de vigilancia debe ser estrictamente necesaria ("*strict necessity*") para la obtención de informaciones vitales en tal operación[211]. La legislación específica debe ser accesible a las personas y comprensible en su significado así como la posibilidad de predecir las consecuencias[212]. En conclusión, el Tribunal de Estrasburgo establece que un gobierno puede interceptar las comunicaciones de un ciudadano sólo si el organismo que autoriza la medida asegura que hay un «*reasonable suspicion*»[213] de la existencia de irregularidades por parte de la persona interesada. Para ser legítima la vigilancia debe estar dirigida, y no puede ser generalizada; es decir, el orden debe identificar claramente a una persona específica[214] o un grupo, y la identificación puede ser hecha por los nombres, direcciones, números de teléfono u otra información específica.

4.3. Exegésis del artículo 8 del CEDH en la jurisprudencia del TEDH respecto a la injerencia en el derecho a la vida privada por los Estados

136. Como se ha visto, el Convenio de Roma ofrece un alto nivel de protección de datos personales. Contrariamente al orden jurídico de la UE (*vid. infra*), el Convenio no afirma la protección de datos personales como un derecho fundamental distinto. Por el contrario, la protección de datos personales forma parte de los derechos protegidos por el derecho al respeto de la vida privada. Por lo tanto, ninguna operación que implique el tratamiento de datos personales podría entrar en el ámbito del artículo 8 del Convenio. Para que se active el artículo 8, primero se debe determinar si un interés privado, o la vida privada de una persona, se ha visto comprometido. A través de su jurisprudencia, el TEDH ha tratado la noción de "vida privada" como un concepto amplio, que abarca incluso aspectos diferentes de la vida de las personas. También ha dictaminado que "la protección de los datos personales es una parte importante del derecho al respeto de la vida privada". Sin embargo, a pesar de la interpretación amplia de la vida privada, no todos los tipos de tratamiento comprometerían los derechos protegidos en virtud del artículo 8 del CEDH. Cuando el TEDH considere que la operación de tratamiento en cuestión afecta el derecho de los

[211] Los jueces, sin embargo, censuran el sistema intrusivo de orden de registro, la interceptación y grabación, que se llevará a cabo tanto físicamente como por la computadora, que la legislación húngara introdujo sin proporcionar garantías adecuadas para la protección de la persona en cuestión.
[212] Ilaria Maria CALAFIORE (2016), «Budapest è solo il più recente caso di una legislazione antiterrorismo accusata in tutto il mondo di essere eccessivamente invasiva o repressiva», en *Eurocomunicazione.com*. Disponible en Internet: http://www.eurocomunicazione.com/lungheria-nuovamente-nel-mirino-delle-istituzioni-la-legge-antiterrorismo-non-salvaguarda-i-diritti-dei-cittadini/ [consulta: 05 de marzo de 2016]
[213] TEDH, *Szabó and Vissy contra Hungría*, conclusiones.
[214] TEDH, *Roman Zakharov contra Rusia*, apartado 264: «(…) *it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information*», y TEDH, *Szabó y Vissy contra Hungría*, apartados 73-75. *Vid*. también TEDH, *Klass y otros contra Alemania*, apartado 51.

individuos a respetar la vida privada, examinará si la interferencia está justificada. El derecho al respeto de "la vida privada no es un derecho absoluto, sino que debe contrapesarse y conciliarse con otros intereses y derechos legítimos, ya sean de otras personas (intereses privados) o de la sociedad en su conjunto (intereses públicos)"[215]. Basado en una interpretación amplia de la noción de vida privada, han sido identificados por el TEDH los principios y sus derechos. De acuerdo con su jurisprudencia, el tratamiento debe realizarse de conformidad con los principios de legalidad, legitimidad, proporcionalidad y temporalidad.

137. Con respecto al requisito de legalidad, según el cual la medida limitativa del derecho al respeto de la vida privada tiene que ser prevista por ley, el TEDH rechazó una noción puramente formal de la ley. La base jurídica se puede encontrar no sólo en una ley escrita, sino también inferir de reglas de la práctica judicial. La existencia de una base jurídica en virtud de la legislación nacional no es suficiente ya que también requiere un cierto nivel de calidad. La norma en cuestión debe respetar el Estado de Derecho: tiene que ser accesible para las personas afectadas y lo suficientemente clara en sus efectos, a fin de que las personas puedan prever las consecuencias y entender lo que se les permite. Por lo tanto, se debe indicar el alcance de discreción atribuido a las autoridades competentes y la forma de su ejercicio con suficiente claridad, a fin de asegurar al individuo una protección adecuada contra la interferencia arbitraria[216].

138. El objetivo legítimo puede ser uno de los intereses públicos mencionados o la protección de los derechos y libertades de los demás[217]. Los objetivos legítimos que podrían justificar una interferencia son, de conformidad con el artículo 8, apartado 2, del CEDH, los intereses de la seguridad nacional, la seguridad pública o el bienestar económico de un país, la prevención del desorden o el delito, la protección de la salud o moral, y la protección de los derechos y libertades de otras personas.

---

[215] «*The right to respect for private life is not an absolute right, but must be balanced against, and reconciled with, other legitimate interests and rights, be they of other persons (private interests) or of society as a whole (public interests)*». *Vid*. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018), *Handbook on European data protection law 2018 edition*, Luxembourg, Publications Office of the European Union, April 2018, págs. 37. El artículo 8, de hecho, contiene la reserva de que los Estados suscritores del CEDH pueden restringir esos derechos, correspondientes al fin de la ley y los objetivos legítimos para garantizar la protección de una sociedad democrática y en los límites que eso sea adecuado y proporcionado a la consecución de dicha finalidad.

[216] TEDH, *Malone contra el Reino Unido*, apartados 66-68; TEDH, *Leander contra Suecia*, apartados 50, 51; TEDH, *Amann contra Suiza* [GS], apartado 50 y 56; TEDH, *Rotaru contra Romania* [GS], apartados 52, 55 y 57; TEDH, *S. and Marper contra Reino Unido*, apartado 95.

[217] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 39).

139. La recogida y tratamiento de datos personales y de comunicaciones debiera producirse sólo cuando «*sea realmente necesario para la salvaguarda de la seguridad*»[218]. Entendemos como "necesidad" como la «*relación directa entre el conocimiento de esa información y la defensa de la seguridad en algún aspecto concreto*»[219]. El propósito de la norma es, de hecho, proteger la dignidad personal del individuo contra la interferencia arbitraria por parte de las autoridades públicas. Pero no sólo basta con que exista una necesidad, sino que hemos de acudir al "principio de proporcionalidad", que «*es el límite de toda injerencia estatal en los derechos fundamentales*»[220]. Es decir, que «*además de perseguir la salvaguarda de la seguridad nacional, sea estrictamente necesario tal control y que no existan medios alternativos menos invasivos para alcanzar la garantía de tal seguridad*»[221]. La proporcionalidad exige que la injerencia en los derechos protegidos por el CEDH "no vaya más allá de lo necesario para alcanzar el objetivo legítimo perseguido"[222]. En otras palabras, los Estados han de abstenerse de interferir en la esfera de privacidad reconocida al individuo. Por esta obligación de carácter negativo también se añade la obligación positiva del Estado miembro de asegurar el respeto efectivo de la vida privada y familiar[223].

[218] Rosario SERRA CRISTÓBAL (2015b), «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», en *UNED. Revista de Derecho Político*, núm. 92, pág. 104. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/14422 [consulta: 16 de noviembre de 2015].

[219] Rosario SERRA CRISTÓBAL (2015b: 104). "Necesidad" no es sinónimo de "indispensable", ni tiene el carácter flexible de los otros, tales como "admisible", "razonable", "útil" y "deseable". En este sentido, *cfr*. Paul DE HERT and Serge GUTWIRTH (2006), «Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power», en Erik CLAES and others (eds.), *Privacy and the Criminal Law*, Antwerp/Oxford, Intersentia, pág. 87. Disponible en Internet: http://works.bepress.com/serge_gutwirth/5/ [consulta: 16 de noviembre de 2015].

[220] Rosario SERRA CRISTÓBAL (2015b: 104).

[221] Rosario SERRA CRISTÓBAL (2015b: 104).

[222] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 40), en particular: «*Proportionality requires that an interference with the rights protected under the ECHR should not go any further than what is needed to fulfil the legitimate aim pursued*».

[223] Por ejemplo, en el caso *X e Y contra los Países Bajos* (en el cual se cuestionaba la legislación holandés en cuanto impedía que el padre de una retrasada mental violada emprendiera acciones penales contra los sospechosos de haber realizado un atentado contra la integridad sexual de su hija), el Tribunal, tras recordar que el artículo 8 del CEDH tiene como objeto proteger a los individuos contra las injerencias ilegítimas de los poderes públicos, interpreta dicho artículo en el sentido de considerar que con éste no se pretende únicamente impedir la injerencia del Estado. En este sentido, el TEDH afirma que a esta obligación negativa de no injerencia pueden añadirse obligaciones positivas inherentes al respeto a la vida privada y familiar, entre las cuales pueden encontrarse la adopción de medidas tendentes a asegurar el respeto de la vida privada, incluso en las relaciones entre los individuos. TEDH, *X e Y contra los Países Bajos*, núm. 8978/80, sentencia de 26 marzo de 1985. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57603#{%22itemid%22:[%22001-57603%22]} [consulta: 02 de junio de 2015].

140. En particular, el TEDH ha reconocido a las disposiciones del CEDH un doble orden de obligaciones a los Estados miembros[224]. Por una parte, existen obligaciones con carácter negativo, que consisten en la prohibición de participar en la interferencia o intromisión en la vida privada[225], en la vida familiar, en el hogar y en la correspondencia de los individuos. Por otra parte, existen obligaciones positivas, que consisten en la obligación de poner en marcha acciones positivas para garantizar la eficacia efectiva de respeto del derecho a la intimidad en virtud del CEDH[226]. Este último tipo de obligaciones pueden dar lugar, en algunos casos, a la adopción de medidas para poner en práctica los derechos de las personas, o, en otros casos, puede consistir en la predisposición de medidas de protección de tales derechos contra la interferencia de los demás.

[224] TEDH, *K.U. contra Finlandia*, núm. 2872/02, apartados 42 y ss. En la misma línea, la sentencia *Haralambie contra Rumania*, en la que el TEDH ha encontrado una violación del derecho al respeto de la vida privada debido a la dificultad de acceso del demandante a un expediente sobre él y que había sido elaborado por los servicios secretos durante el régimen comunista. Según el Tribunal, la cantidad de archivos para ser transferidos y las deficiencias del sistema de almacenamiento no pueden justificar un retraso de varios años con el fin de satisfacer la petición del solicitante. El Tribunal determinó que el Estado parte no había cumplido la obligación positiva de establecer un procedimiento eficaz para el solicitante para consultar dentro de un tiempo razonable en su expediente personal. En este sentido, recuerda que las obligaciones negativas para proteger al individuo contra las injerencias arbitrarias de las autoridades públicas pueden añadirse también obligaciones positivas. El límite entre las obligaciones positivas y negativas en virtud del artículo 8 no se presta a una definición precisa, pero los principios aplicables son comparables. *Vid*. TEDH, *Haralambie contra Rumania*, núm. 21737/03, sentencia de 27 de octubre de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["856690"],"itemid":["001-95302"]} [consulta: 11 de junio de 2015]. David HARRIS, Michael O'BOYLE, Edward BATES, and Carla BUCKLEY (2014: 563).

[225] Si la conducta activa u omisiva por parte del Estado constituye una injerencia en el derecho a la privacidad, esta conducta debe ser justificable o aceptable de acuerdo con las condiciones del apartado segundo artículo 8 del CEDH. Francisco JIMÉNEZ GARCÍA (2014), «La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa», en Eva R. JORDÀ CAPITÁN y Verónica DE PRIEGO FERNÁNDEZ (dirs.), *La protección y seguridad de la persona en internet. Aspectos sociales y jurídicos*, Madrid, Editorial Reus, págs. 49-79.

[226] Consecuencia de esta posición ha sido el reconocimiento, por parte del Tribunal, de que el respeto de los derechos del Convenio implica no solamente que las autoridades públicas deben abstenerse de actuaciones que interfieran indebidamente en el ejercicio de esos derechos, sino también, y adicionalmente, que esas autoridades tienen la obligación de proveer los medios necesarios para la defensa efectiva de los mismos. Y ello tanto en lo que se refiere a vulneraciones causadas directamente por esos poderes públicos, como también en los supuestos en que la inacción de tales poderes se convierte en elemento determinante de esa violación, aun cuando ésta se haya iniciado por actuaciones de terceros particulares. Sobre este punto hay que señalar el caso *Airey contra Irlanda*, núm. 6289/73, sentencia de 9 de octubre de 1979, apartados 32 y 33. *Vid*. María Reyes PÉREZ ALBERDI (2011), «La jurisprudencia social del Tribunal Europeo de Derechos Humanos», en *LEX SOCIAL-Revista de los Derechos Sociales*, núm. 1, págs. 93-105. Disponible en Internet: https://www.upo.es/revistas/index.php/lex_social/article/viewFile/255/250 [consulta: 20 de mayo de 2017]; Luis M. LÓPEZ GUERRA (2013), «El sistema europeo de protección de derechos humanos», en George Rodrigo Bandeira GALINDO, René URUEÑA, Aida TORRES PÉREZ (coords.), *Protección multinivel de derechos humanos. Manual*, Barcelona, Red de Derechos Humanos y Educación Superior, págs. 178-179. Disponible en Internet: http://e-archivo.uc3m.es/handle/10016/19770 [consulta: 20 de mayo de 2017]. También en el *X e Y contra los Países Bajos*, apartado 23: «*The Court recalls that although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves*».

141. Desde la óptica de proporcionalidad, es esencial que exista un equilibrio adecuado entre los derechos en conflicto, de un lado la seguridad pública, por otro lado, los demás derechos fundamentales de los ciudadanos. La proporcionalidad a los objetivos legítimos perseguidos exige evaluar teniendo en cuenta todas las circunstancias del caso, la naturaleza, el alcance y la duración de las medidas que determinan la interferencia, especialmente el número de personas afectadas, las razones que subyacen a la autorización, las autoridades competentes, y el remedio previsto por la legislación nacional[227]. El requisito de proporcionalidad implica la verificación de la posibilidad de llegar a la meta con medios menos invasivos, en cuyo caso la medida de vigilancia resulta desproporcionada[228].

142. En lo que toca a los límites permisibles, el requisito básico es la "previsibilidad" y "accesibilidad" de la ley. La ley, también, debe aclarar los objetivos para los cuales las autoridades pueden recurrir a herramientas invasivas, tales como la vigilancia e interceptación, y ajustar el modo de operación con la precisión suficiente, para dar una protección adecuada a los ciudadanos contra cualquier uso indebido[229]. Resultan admisibles excepciones relativas a la seguridad nacional[230] o la prevención o represión de la delincuencia. A través de este juicio de idoneidad y proporción de la interferencia pública en el derecho de la persona[231], el Tribunal de Estrasburgo ha trazado hasta el momento una

[227] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 40).

[228] En un examen más cercano, podemos recordar la decisión del Tribunal de Justicia de la UE, en declarar inválida la Directiva 2006/24/CE, que parece conforme a lo dispuesto en el artículo 8 del CEDH. En efecto, la sentencia del Tribunal de Justicia se basa precisamente en la evaluación de conformidad con el principio de proporcionalidad entre los métodos de conservación y los fines de datos, aunque legítimo, perseguido por el legislador europeo a través de la adopción de la Directiva. *Vid*. ampliamente el Capítulo IV *infra*.

[229] Matthew RICE (2015), «Zakharov v Russia: A refresher on how far Europe has come», en *Privacy International*, London. Disponible en Internet: https://www.privacyinternational.org/node/688 [consulta: 15 de diciembre de 2015].

[230] El TEDH ha reconocido, en las sentencias *Leander contra Suecia* y *Amann contra Suiza*, que la grabación y trasferencia de datos sobre la vida de una persona, junto con la negación de la posibilidad de acceder, integran una interferencia en la vida privada. Dicha interferencia se considera admisible como prescrito por ley y necesarias en una sociedad democrática en interés de la seguridad nacional (artículo 8, apartado 2). El almacenamiento de los datos por parte de la autoridad pública determina una injerencia en la vida privada de un individuo y la siguiente utilización de la información es irrelevante.

[231] Por lo tanto, en virtud de la adhesión al Convenio, la Unión Europea está también encargada del deber de tomar medidas, mediante el cumplimiento de sus obligaciones positivas en virtud del artículo 8 del CEDH, con la elaboración de las medidas necesarias para proteger la esfera de privacidad de los ciudadanos, incluso mediante la protección de los datos privados y personales de los propios ciudadanos por la interferencia ilegítima y desproporcionada llevado a cabo por otras entidades (entre ellos figuran también los Estados). Es decir, que los Estados no sólo tienen el deber de tomar medidas, mediante el cumplimiento de sus obligaciones positivas en virtud del artículo 8, con las medidas necesarias para proteger la intimidad de los ciudadanos, sino también el deber específico de vigilar que no sean cometidas violaciones de los derechos reconocidos. David HARRIS, Michael O'BOYLE, Edward BATES, and Carla BUCKLEY (2014: 22 y ss.). Entre estas medidas, podemos llamar al control jurisdiccional dentro de cada Estado que tiene como objetivo limitar el poder discrecional de las autoridades reconocidas a dictaminar las medidas de vigilancia, averiguando si existen motivos suficientes para la ejecución de la medida misma. TEDH, *Marckx contra Belgium*, núm. 6833/74, sentencia de 13 junio de 1979. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57534#{%22itemid%22:[%22001-57534%22]} [consulta: 02 de junio de 2015].

trayectoria de procesamiento de la situación jurídica de la persona con respecto a las formas de comunicaciones digitales y las grandes oportunidades que la tecnología de la información ofrece a la hora de almacenar, recoger y difundir datos.

143. El TEDH precisa que hay una prohibición general de injerencia de la autoridad pública en el ejercicio de este derecho, y que tal injerencia es posible si está prevista por ley y constituye una medida que se considera "necesaria en una sociedad democrática"[232], a la seguridad nacional, a la seguridad pública o el bienestar económico del país, a la defensa del orden y a la prevención del delito, a la protección de la salud o la moral, o la protección de los derechos y libertades de los demás, para alcanzar un objetivo legítimo si responde a una "necesidad social acuciante"[233] y, sobre todo, si es proporcionada al fin legítimo perseguido y si los «*motivos invocados por las autoridades nacionales para justificar son "pertinentes y suficientes"*»[234] (legitimidad). Específicamente en relación con los casos examinados anteriormente, resulta pacífico, de acuerdo con la jurisprudencia del Tribunal, que la conservación de los datos personales constituye una injerencia en la vida privada de los individuos, independientemente del posterior uso que se hace de ellos. Esta actividad, por tanto, para ser considerada admisible de conformidad con el artículo 8 del CEDH[235], debe ser prevista legalmente y debe ser necesaria en una sociedad democrática, en el marco del respeto del principio de proporcionalidad[236].

[232] En relación a la jurisprudencia elaborada por el TEDH con los artículos 8 a 11 del CEDH, *vid*. Javier TAJADURA TEJADA (2008), «La doctrina del Tribunal Europeo de Derechos Humanos sobre la prohibición de partidos políticos», en *Boletín Mexicano de Derecho Comparado*, núm. 123, págs. 1431-1475. Disponible en Internet: http://www.revistas.unam.mx/index.php/bmd/article/view/10779 [consulta: 02 de junio de 2015]; Daniel I. GARCÍA SAN JOSÉ (2001), *Los derechos y libertades fundamentales en la sociedad europea del siglo XXI: análisis de la interpretación y aplicación por el Tribunal Europeo de derechos humanos de la cláusula "necesario en una sociedad democrática"*, Sevilla, Universidad de Sevilla, págs. 67 y ss.

[233] Retomando lo comentado antes, el TEDH ha declarado que «*The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued*». *Vid*. TEDH, *Leander contra Suecia*, apartado 58.

[234] *Amplius*, Daniel I. GARCÍA SAN JOSÉ (2001: 82, 75-83). La interferencia debe ser establecida por una disposición normativa que tenga los caracteres de previsibilidad y accesibilidad; perseguir uno o varios de los objetivos legítimos establecidos en la misma («*la seguridad nacional, la seguridad pública, el bienestar económico del país*», etc.); necesaria para satisfacer una "necesidad social imperiosa" y "proporcional" a la consecución de los propósitos legítimos. En comparación con el último principio, la interferencia no debe de ser excesiva, irrazonable o discriminatoria, teniendo también en cuenta la intensidad o la gravedad de la interferencia y garantías judiciales a tutela del individuo.

[235] TEDH, *Amann contra Suiza*, apartado 69: «*The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding*». Gloria GONZÁLEZ FUSTER (2009: 662-663).

[236] Cuando el Tribunal considera un conjunto de acciones y medidas proporcionadas al objetivo declara la no violación del derecho; de lo contrario declara la violación.

144. Según el Tribunal, la ley debería establecer plazos para la autorización de las medidas de vigilancia (temporalidad). También es necesario establecer normas claras que regulen el almacenamiento, uso y divulgación de datos interceptados, reduciendo al mínimo los riesgos de acceso o divulgación no autorizados de los datos. El Tribunal considera que es esencial la previsión de una obligación de cancelación de los datos no pertinentes al objetivo de intervención[237]. Si inicialmente está dentro de la discreción de las autoridades nacionales demostrar que se cumplen estos requisitos, es responsabilidad de la Corte decidir definitivamente la cuestión de la necesidad de cualquier interferencia con los requisitos del Convenio.

145. Por efecto de su actividad, el Tribunal consideró sistemáticamente durante años el Convenio como un «*instrumento vivo*», que tuvo que adaptarse a las cambiantes realidades sociales por medio de una interpretación evolutiva y dinámica[238]. De hecho, el TEDH opera una continua consolidación de los derechos conexos, por cuanto nos interesa, a los cambios en la sociedad y la tecnología, con especial referencia a la amenaza planteada por los Estados a la privacidad, argumentando entre los opuestos criterios del consenso europeo y el margen de apreciación de los Estados[239]. El Tribunal interpreta el texto mediante una interpretación convencional, si es posible, en línea con el consenso europeo[240]. La norma europea aplicable es, en su mayor parte, el resultado de una búsqueda realizada por el Tribunal sobre la existencia de una base común entre la legislación y la práctica de los Estados, en especial con el fin de estrechar el margen de apreciación[241]. Se observa que el Tribunal, como es

[237] Así el TEDH se pronunciaba sobre los juicios *Roman Zakharov contra Rusia* y *Szabó and Vissy contra Hungría*.

[238] *Vid*. Christina BINDER (2015), «El Tribunal Europeo de Derechos Humanos y el Derecho de los Tratados ¿Fragmentación o Unidad?», en *Anuario español de Derecho Internacional*, vol. 31, págs. 307. Traducción del Dr. iur. Henry Jiménez Guanipa. ISBN: 0212-0747. Disponible en Internet: https://www.unav.edu/publicaciones/revistas/index.php/anuario-esp-dcho-internacional/article/viewFile/4623/3985 [consulta: 22 de junio de 2016].

[239] *Vid*. José Antonio PASTOR RIDRUEJO (2007), «La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: temas escogidos», ponencia *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, Madrid, pág. 256. Disponible en Internet: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2007/2007_8.pdf [consulta: 22 de junio de 2016].

[240] Desde este punto de vista, también es claro que, con la transición a la "Sociedad de la Información", el Tribunal, de hecho, ha protegido el derecho a la privacidad en el tratamiento automatizado de datos de carácter personal a través de una interpretación amplia del artículo 8 del CEDH, que ha sido implementado por el legislador de la Unión y se encuentra ahora en el artículo 8 de la Carta de la UE (Protección de datos de carácter personal) y también en el artículo 7 (Respeto de la vida privada y familiar), como un derecho fundamental estrechamente relacionado pero distinto de la protección de datos personales (*vid*. *infra*).

[241] El equilibrio de los intereses generales y particulares del TEDH se realiza mediante criterios, tales como la proporcionalidad de los objetivos perseguidos y la necesidad de excepciones en una sociedad democrática. La acción judicial de la Corte se mantiene en los límites de interferencia en la esfera soberana de los Estados, si se tiene en cuenta, por una parte, la aplicación del principio de proporcionalidad; por el otro, la doctrina pretoriana de margen de apreciación, lo que permite un espacio flexible al Estado, especialmente en la

lógico, ha concedido muchas veces a los Estados un amplio margen de apreciación, tanto con respecto a la decisión de imponer un estado de emergencia, tanto en cuanto a la elección de las medidas excepcionales necesarias para hacerle frente[242]. Desde esta perspectiva, las decisiones del TEDH de dejar a los Estados miembros un amplio margen de apreciación para determinar cuales sean las medidas necesarias parece difícil de justificar, omitiendo al menos en parte su tarea de control[243].

146. Por último, para completar el presente apartado, podemos afirmar que las grandes líneas jurisprudenciales del TEDH sobre la protección de la privacidad y el déficit de seguridad, por referencia especial a la lucha contra la criminalidad, empezó a delimitarse con la sentencia *S. and Marper contra Reino Unido*, de 4 de diciembre de 2008 y, como se ha visto, también recientemente en defensa de un derecho fundamental potencialmente en riesgo como el derecho a la privacidad. Al mismo tiempo, también procedió a dar indicaciones claras de mérito a los legisladores, fijando principios de una manera muy detallada, a fin de permitir su aplicación también en los actos ulteriores adoptados a nivel europeo, como el caso, de hecho, de la nueva normativa europea aprobada en 2016.

147. Desde el examen de las argumentaciones del TEDH en las diversas sentencias en la materia, se pueden deducir diversos requisitos[244], como un *vademécum* "útil" para los Estados a la hora de determinar si es legítima su injerencia en la vida de los individuos: la medida debe ser expresamente prevista por ley; debe ser necesaria en una sociedad democrática para alcanzar el propósito legítimo previsto y debe ser el único medio posible para este fin; debe ser específica y no puede referirse a un conjunto indiscriminado de individuos. La legislación debe prever criterios objetivos por los que determinar los delitos

aplicación concreta de las excepciones a la protección de ciertos derechos. La doctrina jurisprudencial del margen de apreciación viene de lejos en la historia del Tribunal. Fue en efecto con ocasión del caso *Handyside contra el Reino Unido*, resuelto por sentencia de 7 de diciembre de 1976 cuando el Tribunal hizo uso por primera vez. José Antonio PASTOR RIDRUEJO (2007: 247 y ss.).

[242] TEDH, *Irlanda contra Reino Unido*, núm. 5310/71, sentencia de 18 de enero de 1978. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57506#{"itemid":["001-57506"]} [consulta: 25 de junio de 2015]. En doctrina véanse, en particular Rosario SAPIENZA (1991), «Sul margine d'apprezzamento statale nel sistema della Convenzione Europea dei Diritti dell'Uomo», en *Rivista di diritto internazionale*, vol. 74, págs. 571-614. Para una crítica sobre la adopción de la teoría del margen de apreciación, consulte Fionnuala NI AOLAIN and Oren GROSS (2001), «From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights», en *Human Rights Quarterly*, núm. 23, págs. 625-649. Disponible en Internet: http://uir.ulster.ac.uk/15678/ [consulta: 25 de junio de 2015].

[243] David HARRIS, Michael O'BOYLE, Edward BATES, and Carla BUCKLEY (2014: 842).

[244] *Vid*. Bruno SAETTA (2016b), «La sorveglianza di massa in Europa è illegale», en *Valigia blu*, 19 de abril 2016. Disponible en Internet: http://www.valigiablu.it/sorveglianza-illegale-europa/ [consulta: 12 de junio de 2016]; Wojciech R. WIEWIÓROWSKI (2017: 172 y ss.) y Alicia GONZÁLEZ MONJE (2017: 291 y ss.).

que justifican una amplia interferencia con los derechos fundamentales; el acceso a los datos conservados por las autoridades nacionales competentes debe depender de un examen preliminar llevado a cabo por un órgano independiente; el período de retención de datos debe graduarse en función de la posible utilidad para los propósitos alcanzados; deben proporcionarse garantías suficientes contra el riesgo de abuso y el acceso no autorizado y el uso ilícito de los datos guardados; el interesado debe recibir una notificación del hecho de haber sido vigilado, cuando esta comunicación no prejuzgue su vigilancia; y el mismo debe ser capaz de dirigirse a un órgano independiente para hacer cumplir sus derechos.

148. En resumen, de acuerdo con el TEDH, dado el hecho de que un sistema de vigilancia establecido para defender la seguridad nacional es potencialmente capaz de destruir la democracia[245], con el pretexto de defenderla, es esencial que existan garantías adecuadas, y eficaces, contra todas las formas de abuso; y esto debe aplicarse muy en particular a cualquier forma de obtención indiscriminada de datos de los ciudadanos con conservación para futuros propósitos, que por tanto pareciera entenderse que en principio deba ser considerada ilegal.

4.4. El Convenio de Estrasburgo (n. 108) como mínimo nivel básico en la protección de datos en Europa

149. A pesar del papel crucial desempeñado por el artículo 8 del CEDH en la jurisprudencia de la Corte de Estrasburgo que, en virtud de una interpretación dinámica y evolutiva examinada en el apartado anterior[246], ha elaborado las bases para la protección del derecho a la protección de datos personales, aunque no explícitamente, se ha advertido pronto la necesidad de superar la referencia genérica e indeterminada al respeto de la vida privada con un Convenio dedicado específicamente al tema de los datos personales[247].

[245] Bruno SAETTA (2016b).

[246] En el seno del Consejo de Europa, la privacidad como un derecho humano fundamental, recordamos que estamos en el 1950, fue concebido principalmente como protección de la intimidad y destinado a garantizar la protección de datos sensibles. El derecho a la privacidad se ha convertido progresivamente en el derecho a la libre determinación. Significa la posibilidad de que cada uno se determine a sí mismo el camino por el cual le gustaría encontrar su camino en la sociedad. Yves POULLET (2007), «Transborder Data Flows and Extraterritoriality: The European Position», en *3Journal of International Commercial Law and Technology*, vol. 2, issue 3, pág. 142. Disponible en Internet: http://www.jiclt.com/index.php/jiclt/article/view/29/28 [consulta: 15 de junio de 2016]. En el CdE, esta ampliación del derecho a la privacidad desde la protección de datos sensibles al derecho a la autodeterminación se hace por dos vías: en primer lugar, el concepto de privacidad establecido en el artículo 8 del CEDH que se define e interpreta ampliamente por la jurisprudencia del TEDH; en segundo lugar, el CdE adoptó en 1981 el Convenio para la protección de las personas físicas en lo que respecta al tratamiento automatizado de datos personales.

[247] *Vid*. Douwe KORFF (2004), «The legal framework: An analysis of the 'Constitutional' European approach to issues of data protection and law enforcement», en Ian BROWN and Douwe KORFF, *Privacy & Law Enforcement*, UK Information Commissioner study project. En enero de 1968, el CdE adoptó la Recomendación 509 relativa a derechos humanos y desarrollos científicos y tecnológicos. Este instrumento, pone en consideración la problemática que se presenta en relación a los serios daños a los derechos de las

150. La doctrina recordó que las cuestiones problemáticas por resolver eran esencialmente tres[248]: 1) el artículo 8 del CEDH no es aplicable al sector privado, ya que las disposiciones de la Convención dan lugar a obligaciones sólo a los Estados, por lo tanto no puede ser invocado directamente por los particulares contra otros individuos, es decir, no ejerce efectos horizontales en las relaciones entre los individuos; 2) el derecho al respeto de la vida privada no responde necesariamente a todos los datos personales y, consiguientemente, se puso la cuestión de las categorías de datos que se hubieran quedado sin garantías; y 3) el artículo 8 del CEDH no proporcionó un derecho de acceso a sus datos.

151. Antes de seguir adelante, tenemos que recordar que las primeras intervenciones del Consejo de Europa son actos con carácter no vinculante. Entre ellos, son de fundamental importancia la Resolución (73) 22, del Comité de Ministros del Consejo de Europa de 26 de septiembre de 1973 relativa a la protección de la vida privada de las personas físicas frente a los bancos de datos electrónicos en el sector privado; y la Resolución (74) 29 de 20 de septiembre 1974 sobre los bancos de datos en el sector público[249].

152. En ambas Resoluciones se enuncia un breve número de principios fundamentales de protección, acompañados de sendos informes complementarios y aclaratorios. A pesar de su relativa sencillez, estas Resoluciones adquieren una significación histórica: «*son los primeros textos internacionales que presentan a los estados pautas de conducta sobre la protección de los datos personales*»[250]. Desde entonces, en la esfera comunitaria, se abrió pronto el debate sobre la adopción de medidas concretas para frenar los abusos que podían

personas, en concreto al derecho a la privacidad y vida privada, derivado de los avances de la ciencia y los desarrollos tecnológicos. En ese sentido, la Recomendación 509 consiste en que el Comité de Expertos en Derechos Humanos realice un estudio y reporte, con la finalidad de verificar que las legislaciones de los Estados miembros protejan dicho derecho a la privacidad en contra de violaciones que puedan llevarse a cabo a través del uso de métodos científicos y tecnológicos modernos. Gloria GONZÁLEZ FUSTER (2014a), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer International Publishing, vol. 16, págs. 83-84.

[248] *Vid*. Paul DE HERT and Serge GUTWIRTH (2003), «Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies», en *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), págs. 111-162.

[249] Estas Resoluciones, son «*un corto número de principios fundamentales de protección, acompañados de sendos informes complementarios y aclaratorios. A pesar de su relativa modestia, estas Resoluciones adquieren una significación histórica: son los primeros textos internacionales que presentan a los Estados pautas de conducta sobre la materia*». En Gregorio GARZÓN CLARIANA (1981), «La protección de los datos personales y la función normativa del Consejo de Europa», en *Revista de Instituciones Europeas*, vol. 8, núm. 1, pág. 13. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/fondo-historico?IDR=5&IDN=713&IDA=28020 [consulta: 08 de septiembre de 2015].

[250] Mónica ARENAS RAMIRO (2006: 151 y ss.).

producirse tanto en el sector público como en el privado al tratar informaciones personales[251].

153. En realidad, entre los Estados adherentes al Consejo de Europa todavía faltaba una legislación uniforme y, por lo tanto, en presencia de disposiciones heterogéneas, lo que también representaba un obstáculo a la libre circulación transfronteriza de las informaciones. También se destaca que la evolución de las nuevas tecnologías y el flujo intrafronterizo de datos hizo que el CdE detectara la necesidad de una regulación específica del derecho a la protección de datos de carácter personal dentro del derecho a la vida privada.

154. Tras las resoluciones de los años setenta, el Consejo prepara otro instrumento, esta vez vinculante, sobre las formas para almacenar, gestionar y trasladar los datos de carácter personal, respondiendo a la doble necesidad de garantizar la libre circulación de datos, así como la protección de los derechos fundamentales.

155. En concreto, con respecto a los datos personales, el CdE ha actuado al creer insuficiente el artículo 8 del Convenio de 1950, específicamente para proteger a las personas contra los riesgos planteados por la tecnología informática. También, la nueva relación que se ha establecido en la sociedad tecnológica entre los ciudadanos, y entre ellos y el Estado, ha dado lugar a la aparición de una concepción dinámica del derecho a la privacidad, especialmente como derecho al control sobre los datos personales, centrado en particular en la atención a la protección de los datos personales relacionados con la gestión automatizada de los datos. La gestión automatizada de los datos, de hecho, aumentó la cantidad de informaciones disponibles y la privacidad se ha convertido, en primer lugar, en una cuestión de primer orden en el marco de la protección de los datos personales que terminan en

[251] En 1973 un documento interno de la Comisión refleja la inquietud que, con respecto a los derechos de las personas, suscita el empleo de la informática y contempla la necesidad de alcanzar un consenso político que evite futuras divergencias legislativas entre los estados miembros. Igualmente, desde el Parlamento Europeo se interpela al Consejo de las Comunidades Europeas sobre la protección de la vida privada de los ciudadanos comunitarios. A partir de este momento y hasta el comienzo de la década de los ochenta se sucederán otras iniciativas de diversa envergadura (SEC (73) 4300 final, "Una política comunitaria de informática", parágrafo 39; Resolución del Parlamento Europeo de 21 de febrero de 1975, JO n. C 60, de 13/03/1975, pág. 48). En María del Carmen GUERRERO PICÓ (2005), «El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea», en *Revista de Derecho Constitucional Europeo*, núm. 4, págs. 295 y ss. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=1972267 [consulta: 06 de noviembre de 2015]. También recordamos: la Resolución del 8 de mayo de 1979 bajo el título "La protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el sector de la informática", aprobada por el Parlamento Europeo; la Resolución del Parlamento Europeo de 8 de mayo de 1979 sobre "La protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el sector de la informática", DOC. núm. 140, de 5 de junio. En Ana Isabel HERRÁN ORTIZ (1998: 116); María del Carmen GUERRERO PICÓ (2005).

archivos informáticos. Por lo tanto, estos desafíos necesitaban respuestas normativas de carácter internacional más apropiadas y esta necesidad se materializa el 28 de enero de 1981.

156. Los Estados miembros del Consejo de Europa, adoptaron el "Convenio para la protección de las persones con respecto al tratamiento automatizado de datos de carácter personal" (n. 108), comúnmente conocido como el Convenio de Estrasburgo, «(…) *considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras. Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos*»[252].

157. Este Convenio fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos[253]. Aunque todavía desequilibrado del lado de la libertad de información, ha sido a nivel europeo de los primeros intentos para proporcionar un mínimo nivel básico[254] en la protección de datos en Europa[255]. Hay que

[252] Preámbulo del CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, Serie de Tratados Europeos - n. 108, Estrasburgo 28.0I.1981, ratificado por España y publicado en el *Boletín Oficial del Estado* de 15 de noviembre de 1985. Disponible en Internet: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447 [consulta: 13 de junio de 2015].

[253] Cabe señalar que el Convenio n. 108 es vinculante para los Estados que lo han ratificado. No está sujeto a la supervisión judicial del TEDH, pero se ha tenido en cuenta en la jurisprudencia del TEDH en el contexto del artículo 8 del CEDH. A lo largo de los años, el Tribunal ha dictaminado que la protección de datos personales es una parte importante del derecho al respeto de la vida privada (artículo 8) y se ha guiado por los principios del Convenio n. 108 para determinar si ha habido o no interferencia con este derecho fundamental. Ver Abel TÉLLEZ AGUILERA (2002), *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Madrid, Edisofer, págs. 26-58; Mónica ARENAS RAMIRO (2008), «La Protección de datos personales en los países de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 16, págs. 113-168. ISSN 1696-6759. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3057994 [consulta: 14 de junio de 2015].

[254] Los principios de protección de datos contenidos en el Convenio n. 108, que retoma los principios contenidos en las Directrices de la OCDE, se consideran «*estándares mínimos*» para la protección de derechos fundamentales para los países que han ratificado los marcos internacionales de protección de datos. Estos principios deben establecer las bases de cualquier marco de protección de datos y se encuentran en una gran cantidad de leyes de protección de datos, desde la Directiva de la protección de datos de la UE de 1995, y el nuevo RGPD, hasta la mayoría de las leyes de protección de datos en distintos países como en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) en España. Mónica ARENAS RAMIRO (2006: 156 y ss.). Sin embargo, en materia de protección de datos, permitió que los Estados miembros fueran elevando progresivamente su nivel de protección, y de esta forma fue generando un efecto homogeneizador en el sistema de tutela eficaz de estos derechos. Lucrecio REBOLLO DELGADO, María Mercedes SERRANO PÉREZ (2008), *Introducción a la Protección de los datos*, Madrid, Dykynson, pág. 41; Ana Isabel HERRÁN ORTIZ (1998: 193).

[255] Sobre la protección de datos en la Unión Europea, *vid*., entre muchos otros, Lucrecio REBOLLO DELGADO (2014), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson,

señalar que el Convenio falta de una definición de la privacidad o de los derechos, y límites, atribuidos a las personas físicas afectadas.

158. El Convenio n. 108 tiene como fin: «*garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)*» (artículo 1 - Objeto y fin). Su objetivo es garantizar el respeto al derecho fundamental a la protección de datos, por lo que no se trata tanto de limitar la utilización del procesamiento de datos[256], como de "asegurar" y preservar el respeto de los derechos fundamentales de la persona, con especial consideración al derecho a la vida privada bajo siete principios: consentimiento, información, control, calidad, lealtad, seguridad y confidencialidad. También impone normas mínimas a los Estados adherentes, y deja a éstos adoptar normas de aplicación más detalladas.

159. El Convenio n. 108 se aplica a cualquier tratamiento de datos personales dirigido a los individuos[257] y tratamiento automatizado de los datos[258] en el sector privado y en el público, en ese último contexto, también a los realizados por autoridades y policía judicial, permitiendo excepciones a su aplicación en situaciones como la seguridad del Estado. De conformidad con este convenio, los Estados se compromete a adoptar medidas relativas

---

págs. 182; Peter CAREY (2015), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press, págs. 864.

[256] Examinando el objeto de este instrumento internacional, en contraste con lo establecido en el artículo 18, apartado 4, de la Constitución Española, es posible afirmar que los mismo difieren, en cuanto que el texto constitucional proclama de manera explícita la limitación en el uso de la informática para garantizar los derechos y libertades fundamentales. Ana Isabel HERRÁN ORTIZ (1998: 195).

[257] Con respecto a la titularidad de derechos previstos en el Convenio, éste ha sido pensado para la protección de las personas físicas, según lo establece su artículo 2: «*A los efectos del presente Convenio: a) «Datos de carácter personal» significa cualquier información relativa a una persona física identificada o identificable («persona concernida»)*». Sin embargo, es posible, si así lo estipula un Estado parte, proyectar su normativa a la tutela de las personas jurídicas. Se considera que dicha posibilidad, no es irrelevante por la dificultad que plantea extender a las personas jurídicas categorías como las de vida privada o intimidad, que fueron concebidas en función de los intereses de las personas individuales. Antonio Enrique PÉREZ LUÑO (1989), «Los derechos humanos en la sociedad tecnológica», en Antonio E. PÉREZ LUÑO, M.ª Fernanda GUERRERO MATEUS, Mario G. LOSANO, *Libertad informática y leyes de protección de datos personales*, Cuadernos y Debates, Madrid, Centro de Estudios Constitucionales, núm. 21, págs. 135-213; Antonio ORTÍ VALLEJO (1994), «El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio)», en *Derecho Privado y Constitución*, núm. 2, págs. 305-332. Disponible en Internet: http://www.cepc.gob.es/gl/publicaci%C3%B3ns/revistas/revistas-electronicas?IDR=7&IDN=376&IDA=9889 [consulta: 18 de junio de 2015].

[258] Se trata, según cierta doctrina, de una falta común en la mayoría de las medidas normativas de la época, que tienen el objetivo común de contemplar sólo a la protección de los datos personales incluidos en obtenciones automatizadas. Es importante señalar que se habla de un verdadero "síndrome de ordenador". Roberto PARDOLESI (2003) (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, pág. 34.

adecuadas para dar efecto a los principios fundamentales que forman el núcleo duro. Se protege al individuo contra los abusos que pueden acompañar la recogida y el tratamiento de los datos personales y, al mismo tiempo, trata de regular el flujo transfronterizo de datos personales[259]. Está claro, pues, que la protección de datos personales, además de encontrarse en el centro del derecho a la vida privada, tiene más probabilidades de ser violada debido a la facilidad con que esto puede ocurrir con las nuevas tecnologías.

160. En cuanto a la obtención y el tratamiento de los datos personales, los principios establecidos en el Convenio n. 108 exigen que los datos se obtengan y procesen de forma, en particular, "leal y legal", archivados con fines "determinadas y legítimos", y "no para su uso incompatible con tales fines", "ni guardados más tiempo del necesario". Estos principios también conciernen la calidad de los datos, en particular, respecto a su idoneidad, pertinencia y no excedencia (proporcionalidad) y precisión[260]: «*los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado*» (artículo 5 - Calidad de los datos). Los principios establecidos en el artículo 5, letra b), del Convenio forman parte del marco principal de la legislación europea en materia de protección de datos, el llamado "principio de limitación de finalidad"[261].

161. El artículo 5 examina si los sistemas a través de los cuales la UE ha ido ampliando de manera gradual el uso de información personal, para finalidades policiales, pueden vulnerar los principios de necesidad y limitación de finalidad como parte del derecho de protección de datos de la UE. La necesidad de garantías es mayor cuando, sin duda, la protección de datos personales se refiere a los propósitos de policía, como asimismo, al

[259] CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, artículo 3 (Campos de aplicación).
[260] David I. BAINBRIDGE, Nick PLATTEN (1996), *EC Data Protection Directive*, London, Butterworths, págs. 17 y ss.
[261] También el mismo principio se contemplaba en el artículo 6, apartado 1, letra b), de la Directiva de protección de datos de 1995 y en el artículo 3 de la Decisión Marco del Consejo 2008/977/JAI (*vid*. *infra*). Hoy se reconoce en el Reglamento General de Protección de Datos, artículo 5, apartado 1, *vid. infra*.

posible uso de la informática combinada con otras técnicas (por ej.: ADN, datos dactiloscópicos, *etc*.)[262].

162. De acuerdo con el propósito del artículo 5 del Convenio n. 108, el Consejo de Europa, para desarrollar el contenido del Convenio[263], dictó la Recomendación n. R (87) 15 del Comité de Ministros a los Estados miembros, dirigida a orientar a los gobiernos de los Estados miembros a la hora de regular la utilización de datos de carácter personal en el sector

[262] En los últimos años, los perfiles de ADN han proporcionado, sin duda, una contribución importante a las autoridades judiciales en la lucha contra la delincuencia, sin embargo, la protección de los datos personales es de importancia fundamental para aprovechar del derecho al respeto de la vida privada (artículo 8, apartado1, del CEDH). Según el TEDH (para todos se señala *S. and Marper contra Reino Unido*) la lucha contra la delincuencia, especialmente la delincuencia organizada y el terrorismo, constituye uno de los retos más importantes con el que tiene que enfrentarse la sociedad moderna. El éxito de esta lucha depende en gran medida de la utilización de las técnicas científicas más modernas de investigación e identificación. Si bien la Corte reconoció la importancia del papel desempeñado por estas nuevas tecnologías en la identificación de los delitos, por otra parte, tiene la obligación de definir el alcance de su uso. Conservar la información relativa a las huellas dactilares y los datos genéticos persigue el objetivo legítimo de detectar y prevenir la comisión de delitos. Por lo tanto, la conservación de las muestras de células y sus perfiles de ADN constituye una interferencia en el derecho al respeto de su vida privada en el marco del Convenio Europeo. Sin embargo, a las autoridades nacionales competentes debe de ser reconocido un cierto margen de apreciación. Tal margen puede depender de la naturaleza de los derechos convencionales en cuestión, de su importancia para los individuos, de la naturaleza de la interferencia y los objetivos perseguidos por la misma. El margen de apreciación reconocido al Estado se reduce necesariamente cuando el derecho en cuestión es indispensable para el goce efectivo de los derechos fundamentales reconocidos al individuo.

[263] El Consejo de Europa se ha ido desplegando a través de distintas recomendaciones sectoriales dirigidas a los gobiernos de los Estados miembros sobre temas específicos. Siempre en el ámbito del Consejo de Europa, de interés por nuestra investigación son otros dos documentos: la Recomendación n. R (95) 4 del Comité de Ministros del Consejo de Europa en materia jurídica a los Estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos; y la Resolución del Consejo de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones. La Recomendación prevé que las interferencias en las comunicaciones, incluido el uso de instrumentos de escucha o interceptación u otros instrumentos de vigilancia, son elegibles solamente si es requerido por la ley y constituya una medida necesaria en una sociedad democrática para proteger la seguridad pública, la salud pública, los intereses económicos del Estado y para la prevención de delitos. En cualquier caso, el Estado debe garantizar la posibilidad de acceso a los datos y el derecho de rectificación, y la posibilidad de recurrir a un organismo independiente en caso de denegación de acceso o corrección. La Resolución de 1995 del Consejo de Europa, recoge los requisitos para la interceptación legal de los servicios de telecomunicaciones, con sujeción a los requisitos de la legislación nacional. Según la legislación, las autoridades competentes requieren que las telecomunicaciones sean hechas accesibles, pero no se pueden enviar las telecomunicaciones no incluidas en la autorización para la interceptación. Requieren la posibilidad para operar los controles permanentes en tiempo real, para la interceptación de las telecomunicaciones. En el caso de que ellos no puedan ponerse a disposición en tiempo real, las autoridades competentes requieren de su disposición tan pronto sea posible tras el final de la llamada. Las autoridades competentes necesitan que la interceptación se proyecte y lleve a cabo de tal manera «*que sea imposible cualquier uso indebido o no autorizado y que se protejan las informaciones relativas a la interceptación*». *Vid*. RECOMENDACIÓN N. R (95) 4 DEL COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos (Adoptada por el Comité de Ministros el 7 de febrero de 1995, durante la 528ª reunión de los Delegados de los Ministros). Disponible en Internet: http://www.informatica-juridica.com/anexos/recomendacion-no-r-95-4-del-comite-de-ministros-del-consejo-de-europa-en-materia-juridica-a-los-estados-miembros-sobre-la-proteccion-de-los-datos-de-caracter-personal-en-el-ambito-de-los-servicios-de/ [consulta: 29 de junio de 2015]; y RESOLUCIÓN DEL CONSEJO DE 17 DE ENERO DE 1995 sobre la interceptación legal de las telecomunicaciones, *Diario Oficial n° C 329 de 04/11/1996 p. 0001 – 0006*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31996G1104 [consulta: 29 de junio de 2015].

de la policía[264]. La Recomendación tiene por objeto «*servir de guía para el derecho interno de los Estados miembros y la práctica policial en lo relativo a la aplicación de los principios esenciales para la recogida, almacenamiento, uso y comunicación de datos personales con fines policiales, garantizando, a la vez, los derechos relativos a la protección de la intimidad y datos personales de los particulares*»[265]. Por consiguiente, dado que el tratamiento de datos por parte de las autoridades policiales puede tener un impacto significativo sobre las personas afectadas, es especialmente necesario que existan normas detalladas en materia de protección de datos para el correcto mantenimiento de las bases de datos en ese ámbito[266]. La legislación debe asegurar que estos datos sean pertinentes y que no excedan de los fines para los que se almacenan; también deben ser conservados en una forma que permita la identificación de los datos por un período no superior a lo necesario para las finalidades en las que estén registrados[267]. La legislación también debe contener salvaguardias adecuadas para prevenir el abuso y el mal uso de los datos personales guardados.

163. La Recomendación de 1987 establece que la recogida de datos con fines policiales debe limitarse a los datos necesarios para la prevención de un «*peligro concreto*» y la represión de los delitos específicos[268]. La Recomendación no permite una recopilación de datos abierta e indiscriminada[269] por parte de las autoridades policiales. Por otro lado, en caso de que los datos personales hayan sido recogidos y registrados, el titular debería ser informado en cuanto tal comunicación no pueda dañar a las investigaciones en curso. La comunicación a otros organismos públicos debería ser permitida sólo si hay una norma o una autorización específica o si estos datos son esenciales para la prevención de amenazas inminentes. Las restricciones al derecho de acceso a los datos, o el derecho de rectificación o cancelación, deberían limitarse a los casos en que tales límites son necesarios para fines policiales, y en todo caso el sujeto tiene que poder recurrir a una autoridad independiente

[264] *Vid*. RECOMMENDATION REC(87)15 to member states regulating the use of personal data in the police sector, Strasbourg, 17 September 1987; MINISTERIO DE JUSTICIA (1992), *Recomendaciones y resoluciones del Comité de Ministros del Consejo de Europa en materia jurídica*, Madrid, págs. 492 y ss.
[265] Alejandro Luis GACITÚA ESPÓSITO (2014: 142); Olga ESTADELLA YUSTE (1995), *La protección de la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, pág. 66; Emilio ACED FÉLEZ (2010a), «La protección de datos en la cooperación policial europea: de la Recomendación (87) 15 al principio de disponibilidad. Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. Artículos 22, 23.1 y 24.1», en Antonio TRONCOSO REIGADA (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, págs. 1350-1388. ISBN 978-84-470-3423-9.
[266] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 277).
[267] Principio 6 (Publicidad, derecho de acceso a los ficheros policiales, derecho de rectificación y derecho de recurso) y Principio 7 (Período de conservación y actualización de los datos). MINISTERIO DE JUSTICIA (1992: 499-500).
[268] Principio 2.1 (Recogida de datos). MINISTERIO DE JUSTICIA (1992: 495).
[269] *Vid*. AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 164).

que garantice la legitimidad de la denegación[270]. Dicha Recomendación constituye una de las disposiciones normativas más relevantes elaboradas por la UE concerniente el específico tratamiento de datos personales para fines de represión y prevención penal.

164. Otro artículo del Convenio n. 108, que ofrece garantías sobre la recogida y el tratamiento de los datos personales, prohíbe el tratamiento de datos "sensibles" en ausencia de garantías jurídicas adecuadas, y ofrece una respuesta a los crecientes temores de perfiles indiscriminados de los aspectos más íntimos de las personas o actitudes discriminatorias basadas en datos características, como la raza, las opiniones políticas, la salud, la religión, la orientación sexual o las condenas penales de un individuo. En particular, en el artículo 6 (Categorías particulares de datos) se establece que: «*Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales*». En este artículo se prohíbe el tratamiento automatizado de estos datos[271], a menos que la legislación nacional no introduzca "garantías apropiadas". La identificación de estas últimas se deja a los Estados miembros[272].

165. El Convenio, como el resto de los instrumentos examinados hasta aquí, prevén como es lógico excepciones al derecho a la protección de datos personales. Los Estados pueden, de acuerdo con el artículo 9 (Excepción y restricciones), mitigar tanto las obligaciones y los derechos previstos en el acuerdo internacional. La ley interna del país adherente, de hecho, podrán establecer excepciones a las disposiciones contenidas en el Convenio, siempre que

[270] Principio 6 (Publicidad, derecho de acceso a los ficheros policiales, derecho de rectificación y derecho de recurso). MINISTERIO DE JUSTICIA (1992); EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 277-279).

[271] Los artículos apenas llamados, en particular nos referimos a los artículos 5 y 6 del Convenio, establecen elementos que parecen, sin duda, apropiados para ponerse de manera vaga en conflicto con la transferencia de datos, con la conservación y utilización de los datos contenidos en los *PNR* o transaccional financiera internacional, aunque a beneficio de las situaciones de interés general, como la seguridad colectiva y la lucha contra los fenómenos terroristas.

[272] Otro principio, que no parece ser de ninguna manera derogable, se relaciona con el artículo 7 (Seguridad de los datos) del Convenio n. 108. Este artículo establece que los países, son llamados también a prever las "medidas de seguridad" que impiden que las formas de destrucción y la pérdida accidental de datos registrados, y que, en cualquier caso, evitan el acceso no autorizado y la difusión de los mismos: «*se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados*». Se trata de un deber de los Estados para establecer la obligación para los responsables del trato que tendrán que adoptar garantías adecuadas al tipo de tratamiento, el nivel de riesgo y el estado de los conocimientos informáticos.

tal excepción «*constituya una medida necesaria en una sociedad democrática: a) para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de otras personas*» (artículo 9, apartado 2). La excepción debe ser establecida por la ley.

166. Con esta disposición, el Consejo ha reproducido fielmente las disposiciones ya previstas por el apartado segundo del artículo 8 del CEDH por el derecho al respeto a la vida privada y familiar[273]. Se trata de una lista exhaustiva diseñada para evitar que los países firmantes puedan tener un margen demasiado amplio de maniobra: «*todas las excepciones y limitaciones a estos principios fundamentales deberán establecerse a escala nacional; deberán ser establecidas por la ley; servir a un fin legítimo y ser necesarias en una sociedad democrática. Deben cumplirse las tres condiciones*»[274]. Sin embargo, hay que señalar que la interpretación de estas excepciones se deja a la discreción de las Partes contratantes, con consecuencias importantes sobre el nivel real de protección garantizado en cada Estado firmante. A este respecto, el control del TEDH se ha revelado esencial para perfilar el alcance del Convenio n. 108[275], dado que las garantías que éste establece, en particular respecto a la calidad de los datos, categorías particulares de datos y garantías complementarias para la persona concernidas, en los artículos 5, 6 y 8[276], pueden ser objeto de excepciones y restricciones a tenor del artículo 9, apartado 2[277] propio del Convenio.

[273] *Vid*. *supra*.
[274] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 68).
[275] Pues, en efecto, en la sentencia *S. and Marper contra Reino Unido* el TEDH refuerza la interpretación del CEDH tanto con textos programáticos o no vinculantes (como la Recomendación n. R (87) 15 del Comité de Ministros a los Estados miembros) como con instrumentos obligatorios o vinculantes, especialmente el Convenio n. 108.
[276] Entre las medidas convencionales de especial importancia, el Convenio reconoce a sus titulares, cuando la información sea almacenada en bases de datos, a ser informados tanto sobre la existencia, tanto para la obtención electrónica, así como la identidad, el domicilio o residencia del responsable de la misma. El reconocimiento de estos derechos implica el derecho a ser capaz de apelar ante las autoridades competentes en caso de infracción. En particular, el artículo 8 establece que cualquier persona tiene el derecho a «*conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero*» y el derecho a obtener la rectificación o cancelación de sus datos si han sido tratados en violación de las disposiciones. Y, por último, para hacer estos derechos posibles, el derecho a disponer un procedimiento de recurso (acción administrativa o judicial) para la protección de sus derechos en relación a los datos recogidos y almacenados.
[277] Para entender esta expresión jurídica es necesario hacer referencia a la conformidad del tratamiento de la legislación nacional de referencia. Dicha legislación debe respetar el principio de la interferencia justificada en virtud del CEDH, como la interpretación por la jurisprudencia del TEDH, así como las condiciones de las limitaciones legítimas de conformidad con el artículo 52 de la Carta de los Derechos Fundamentales de la Unión Europea (*vid*. *infra*).

167. Al objetivo de armonización de las legislaciones de los países miembros (artículo 12 - Flujos transfronterizos de datos de carácter personal y el derecho interno) se unió la intención que persigue el Convenio para crear entre ellos un espacio de libre circulación de datos: «*las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento*» (apartado 1). Por esta razón, «*una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte*» (apartado 2).

168. Siguiendo con el mismo artículo, no se puede permitir a terceros países la transmisión de los datos personales, cuando no prestan suficientes garantías de protección: «*sin embargo, cualquier Parte tendrá la facultad de establecer una excepción* (…) *en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente* (…)*; cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo*» (apartado 3).

169. El marco abarca la transferencia de datos tanto electrónica como físicamente más allá de la frontera, y menciona específicamente también la simple recopilación de datos destinados a evitar el fenómeno de la exportación automática de los mismos a los "paraísos informáticos". Se prevé la facultad de "derogación" del libre flujo de informaciones tanto en el caso de que la legislación de un Estado contenga una regulación particular para algunas categorías de datos (es decir, sensible) o para determinados sectores (telecomunicaciones, *marketing*), como cuando el Estado destinatario no proporcione una protección equivalente: el grado de protección equivalente depende del nivel de rigurosidad de las legislaciones nacionales del país importador. La facultad del legislador para extender la derogación también se aplica a los casos en los que el flujo de datos dirigido a una parte constituya en realidad un medio para exportar datos a un tercer País no contrayente. De hecho, esta última disposición es la única restricción contenida en el Convenio a la transferencia de datos hacia países no contrayentes. De lo contrario, la Directiva 95/46/CE y ahora el nuevo Reglamento europeo de protección de datos contienen una disciplina más

estricta sobre el punto (*vid*. *infra*), exigiendo a los Estados miembros regular también el traslado de los datos fuera de la UE.

170. El Convenio de Estrasburgo no es un instrumento "*self-executing*", o de ejecución inmediata, pero obliga a las Partes a adecuar sus normativas nacionales al contenido de este instrumento, para lo cual se requieren medidas adecuadas para su implementación (artículo 4 - Compromisos de las Partes).[278] De lo contrario, éste no podrá ser aplicado directamente por los Tribunales[279]. Estas medidas, en aplicación del artículo 22 del Convenio n. 108, deben adoptarse en el momento de la ratificación o más tarde en el momento en que el Convenio entre en vigor para cada Estado[280]. Todos los Estados miembros de la UE han

[278] La naturaleza de las disposiciones del Tratado de no ejecución inmediata es confirmada por el tenor indeterminado de muchas previsiones, por ejemplo, en el artículo 8 que no establece procedimientos, términos y autoridad competente para el ejercicio de los derechos de acceso, rectificación y cancelación, postulando una obra de aclaración al nivel de la legislación nacional. *Vid*. Paolo PALLARO (2002), *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffrè, pág. 53. En este sentido el Convenio n. 108 crea un nuevo órgano: un Comité Consultivo que mediante propuestas mejore la aplicación o presente propuestas de enmiendas, con miras a facilitar o mejorar la aplicación del Convenio, al tiempo que toma parte en la labor normativa, redactando documentos que son generalmente aplicables. *Vid*. CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, Capítulo V.

[279] Alfonso ORTEGA GIMÉNEZ (2015: 50). Esta falta de vinculación inmediata del Convenio ha sido criticada, pues mientras un Estado firmante del mismo no dicte las disposiciones de desarrollo del Convenio, éste no puede ser objeto de aplicación directa por los tribunales. En este sentido, la STC de 20 julio 1993 (BOE de 18 agosto 1993), aunque otorgó el amparo solicitado, lo hizo en virtud de la "eficacia directa" del derecho a la intimidad recogido en el artículo 18 Constitución Española, y no en base a una aplicación inmediata del Convenio de 1981. *Vid*. Javier CARRASCOSA GONZÁLEZ (1997), «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, págs. 509-539. Disponible en Internet: http://www.academia.edu/11583471/Circulaci%C3%B3n_internacional_de_datos_personales_informatizados_y_la_Directiva_95_46_CE [consulta: 9 de julio de 2015]; Carlos RUÍZ MIGUEL (2003), «El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, págs. 7-43. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=635290 [consulta: 9 de julio de 2015]; y Antonio TRONCOSO REIGADA (2010: 57).

[280] España ratificó el Convenio n. 108 el 31 de enero de 1984, pero no fue hasta la promulgación de la LORTAD (Ley 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal), cuando el País cumplió con sus obligaciones jurídico-internacionales establecidas en el texto normativo, referidas precisamente a la elaboración de la mencionada legislación interna y explicitadas en el artículo 4 del Convenio. En este sentido, Santiago RIPOLL CARULLA (1990), «En torno a la calificación de la pasividad española en el cumplimiento del Convenio nº 108 de Europa como acto ilícito internacional», en *La Responsabilidad Internacional*, XIII Jornadas de la AEPDIRI, Alicante, págs. 313-330. También *vid*. Juan Antonio PAVÓN PÉREZ (2001: 239). Italia ratificó el Convenio de Estrasburgo con un retraso considerable por la Legge 21 febbraio 1989, n. 98. *Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981, (GU Serie Generale n. 66 del 20-03-1989 - Suppl. Ordinario n. 19), entrata in vigore della legge 21/3/1989*. El Convenio, a diferencia de otros convenios del Consejo de Europa, tiene carácter abierto, en el sentido de que, una vez en vigor, es accesible a cualquier otro Estado que no sea miembro del Consejo siempre que haya sido invitado a adherirse por el Comité de Ministros. Giovanni BUTTARELLI (1997), *Banche dati e tutela della riservatezza*, Milano, Giuffrè, 1997, págs. 3 y ss.

ratificado el Convenio n. 108[281], que en 1999 fue modificado para permitir que la UE se conviertiera en Parte[282].

171. No obstante, la enorme importancia del Convenio n. 108 en el establecimiento de una serie de principios de obligado cumplimiento en materia de protección de datos de carácter personal, transcurridos 20 años desde su adopción y la irrupción de otros instrumentos posteriores, como la Directiva 95/46/CE (*vid*. *infra*), exigía la adaptación de algunas de las previsiones del Convenio al régimen existente tras la adopción de la Directiva de 1995[283]. El 8 de noviembre 2001 se abrió así a la firma un Protocolo Adicional, para modificar el Convenio n. 108, que entró en vigor el 1 de julio de 2004. El acuerdo se ha enriquecido de esta forma de dos previsiones especialmente relevantes[284].

172. En cuanto a su articulado, el artículo primero dispone que las Partes en el Convenio deberán establecer una o varias autoridades independientes[285] con el objetivo de asegurar el respeto de los principios enunciados en el mismo. Estas autoridades de control tienen el poder de investigar e intervenir, de interponer una acción judicial o de poner en conocimiento de las autoridades judiciales las violaciones de la legislación sobre la protección de datos. El poder de la intervención puede adoptar diversas formas en el derecho interno, siendo ejemplo

[281] La ratificación por parte de España del Convenio n. 108 ha tenido una importante incidencia en el sistema jurídico español. Esto se ve justificado constitucionalmente, ya que por imperio del artículo 96, apartado 1, de la Constitución Española de 1978, los Tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Cumplidos ambos requisitos, el texto del Convenio Europeo, forma parte del sistema jurídico español, y hasta el año 1982, constituyó la norma básica en materia de protección de datos personales frente a los abusos cometidos en su procesamiento informático. Antonio Enrique PÉREZ LUÑO (1989: 163 y ss.). La ratificación del Convenio n. 108 representó, sin duda alguna, un avance positivo en materia de protección de datos para el ordenamiento español, en tanto que facilitó la efectividad y aplicación plena del texto bajo los auspicios del Comité Consultivo, que ha cuidado y velado por la correcta aplicación de aquél a través de la formulación de propuestas y dictámenes, ya sea de oficio o a instancia de parte, si bien en España su aplicación se hallaba condicionada a la efectiva elaboración de una legislación que posibilitara la plena efectividad de las medidas protectoras, que en el citado Convenio se reconocían. Manuel HEREDERO HIGUERAS (1994), «La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal», en VV.AA., *Informática judicial y protección de datos*, Victoria-Gasteiz, Departamento de Justicia del Gobierno Vasco.

[282] Consejo de Europa, Modificaciones del Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (CETS n. 108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros, en Estrasburgo, el 15 de junio de 1999; artículo 23, apartado 2, del Convenio n. 108 en su forma modificada. *Vid*. AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 17).

[283] Los principios del Convenio han sido el fundamento de la posterior regulación de la privacidad en Europa, y más allá. Sin embargo, el Convenio n. 108 tiene un problema fundamental que se refiere a la aplicabilidad del propio Convenio y del tratamiento internacional de datos. David I. BAINBRIDGE, Nick PLATTEN (1996: 17).

[284] PROTOCOLO ADICIONAL AL CONVENIO para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de control y a los flujos transfronterizos de datos, Estrasburgo, 8 de noviembre de 2001. Disponible en Internet: https://rm.coe.int/16806caea0 [consulta: 13 de junio de 2015].

[285] PROTOCOLO ADICIONAL AL CONVENIO, artículo 1 (Autoridades de control).

de ello cuando la autoridad obliga al responsable del fichero a rectificar, borrar o destruir datos inexactos o recolectados ilícitamente; cuando emite medidas cautelares o dictámenes previos a la ejecución de las operaciones de tratamiento de datos; o cuando remite casos a los Parlamentos nacionales u otras instituciones del Estado. El artículo primero del Protocolo Adicional trata asimismo la independencia de las Autoridades de control.

173. El artículo segundo del Protocolo Adicional, referente a las garantías para proteger el movimiento transfronterizo de datos hacia terceros países, establece como principio general básico, que «*la transferencia internacional de datos personales desde un País miembro del CdE a un tercer Estado u organización internacional que no sea miembro del mismo*»[286], debe efectuarse «*únicamente si dicho Estado u organización asegura un adecuado nivel de protección*»[287]. En realidad, este último principio general está muy mitigado. A las Partes del Convenio se les reconoce la posibilidad de «*autorizar transferencias de datos personales*»[288], a destinatarios no sometidos a la competencia de las Partes del Convenio que no posean un nivel adecuado de protección, en dos casos: «*si el derecho interno así lo establece a causa de: - intereses concretos del afectado, o - intereses legítimos, especialmente los de carácter público*»[289] (entre ellos, por ejemplo: seguridad nacional, seguridad pública, *etc*.). Por último, también se permite la transferencia a Estados u organización que no es Parte del Convenio que no garantizan un nivel adecuado de protección «*si se prevén las suficientes garantías, que pueden resultar, en particular, de cláusulas contractuales, por parte del responsable del tratamiento responsable de la transferencia y dichas garantías se estiman adecuadas por las autoridades competentes de conformidad con el derecho interno*»[290].

174. Los cambios drásticos que se han producido en el escenario tecnológico tras la adopción del Convenio han dirigido el CdE a abrir una consulta pública en 2011[291], para

[286] Alejandro Luis GACITÚA ESPÓSITO (2014: 137).
[287] PROTOCOLO ADICIONAL AL CONVENIO, artículo 2 (Flujos transfronterizos de datos de carácter personal hacia un destinatario que no está sujeto a la jurisdicción de una Parte en el Convenio): «*1. Cada Parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección*».
[288] PROTOCOLO ADICIONAL AL CONVENIO, artículo 2, apartado 2.
[289] PROTOCOLO ADICIONAL AL CONVENIO, artículo 2, apartado 2, letra a).
[290] PROTOCOLO ADICIONAL AL CONVENIO, artículo 2, apartado 2, letra b).
[291] A la víspera de los 30 años de su adopción en 1981, se iniciaron los trabajos preparatorios de la revisión del Convenio n. 108 del Consejo de Europa, aunque ésta se lanzó formalmente a finales de 2010 con la aprobación por el Comité de Ministros de una "Resolución sobre la Protección de Datos y la Privacidad en el Tercer Milenio". En 2011, el Consejo de Europa publicó una hoja de ruta con los hitos principales en lo relativo al proceso de modernización del Convenio n. 108. El Comité Consultivo del Convenio n. 108 elaboró un

estimular un debate sobre las cuestiones más importantes en vista de la modernización del Convenio, confirmando dos objetivos principales de trabajo: el fortalecimiento de la protección de la intimidad en el sector digital y la consolidación del mecanismo de aplicación del Convenio[292]. Después de un largo proceso iniciado en 2011, el Comité de Ministros del Consejo de Europa ha completado el proceso de modernización del Convenio n. 108 de 1981[293].

175. El proceso de modernización del Convenio n. 108[294] tiene como objetivos fundamentales reforzar la protección al abordar nuevos retos y fortalecer los mecanismos de seguimiento, pretendiendo que se promueva como un estándar universal, al ser una herramienta con un carácter sencillo, flexible y pragmático, que garantiza la coherencia y compatibilidad con otros marcos normativos, en especial el nuevo Reglamento General de Protección de Datos. Reafirma y estabiliza principios importantes y proporciona nuevos derechos a las personas, en comparación con el original. En particular, estas son las novedades de mayor impacto[295]: "el fortalecimiento de las obligaciones de transparencia para los responsables de datos"; "la extensión de los derechos de los interesados, que ahora también incluye el derecho a no estar sujeto a decisiones puramente automatizadas y a conocer la lógica del procesamiento"; "mayores garantías para la seguridad de los datos,

documento técnico de reforma que remitió al Consejo de Ministros del Consejo de Europa. Este documento está siendo estudiado por un Comité *ad hoc* (CAHDATA), un grupo de expertos creado en el Comité de Ministros del Consejo de Europa, sobre la adopción y aprobación del proyecto de reforma por este último. *Vid*. Alfonso ORTEGA GIMÉNEZ (2015: 37-56); Graham GREENLEAF (2013a), «Modernising data protection Convention 108: A safe basis for a global privacy treaty?», en *Computer Law & Security Review*, vol. 29, págs. 12. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262296 [consulta: 18 de junio de 2015]; Paul DE HERT, Vagelis PAPAKONSTANTINOU (2014a), «The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition», en *Computer Law & Security Review*, vol. 30, issue 6, págs. 633-642; Cécile DE TERWANGNE (2014), «The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data», en *International Review of Law, Computers & Technology*, vol. 28, issue 2, págs. 118-130.

[292] El Convenio n. 108, como comentado, está abierto a la adhesión de Estados no miembros del Consejo de Europa, y también incluye países fuera de Europa. Uruguay es el primer país no europeo, que se ha adherido en agosto de 2013. *Vid*. Graham GREENLEAF (2013b), «Uruguay starts Convention 108's global journey with accession», en *Privacy Laws & Business International Report*, issue 122, págs. 7. Disponible en Internet: http://ssrn.com/abstract=2280121 [consulta: 20 de junio de 2015]. El autor, en particular, hizo hincapié en que el Convenio n. 108, gracias a la futura adhesión de países no europeos, puede establecerse como Tratado que rige la privacidad internacional, a diferencia de la disciplina europea, sin embargo, que opera en un contexto regional.

[293] La adopción formal tuvo lugar con motivo de la Ministerial de Elsinore, Dinamarca, el 18 de mayo de 2018. El Protocolo de las enmiendas, que actualiza la 108 Convención, estará abierto a la firma el 25 de junio, durante la sesión de la Asamblea Parlamentaria del Consejo de Europa.

[294] Modernisation of Convention 108. Disponible en Internet: https://www.coe.int/en/web/data-protection/convention108/modernised [consulta: 19 de abril de 2019].

[295] Graham GREENLEAF (2016), «Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives», en *142 Privacy Laws & Business International Report*, 14-17; *UNSW Law Research Paper*, núm. 17-3, págs. 9. Disponible en Internet: https://ssrn.com/abstract=2892947 [consulta: 20 de mayo de 2017]; María Belén SÁNCHEZ GONZÁLEZ (2016: 40-44).

incluida la obligación de notificar infracciones de datos ("*data breach*"), y para garantizar un enfoque de privacidad por diseño ("*privacy by design*")". El Protocolo[296] también fortalece las tareas de las autoridades de control de protección de datos y el Comité de la Convención, llamados a desempeñar un papel en la evaluación del respeto efectivo de los principios de la Convención que deben garantizar los países que formarán parte de ella.

176. Con respecto a la policía y la justicia penal, a nivel europeo, el Convenio modernizado 108 cubre todas las áreas del procesamiento de datos personales, y sus normas tienen por objeto regular el procesamiento de datos personales en general. En consecuencia, "el Convenio modernizado 108 se aplica a la protección de datos en el área de la policía y la justicia penal". El procesamiento de datos genéticos, datos personales relacionados con delitos, procesos penales y condenas y cualquier medida de seguridad relacionada, datos biométricos que identifiquen de manera única a una persona, así como cualquier dato personal sensible, sólo se permite cuando existan salvaguardas adecuadas contra los riesgos que el tratamiento de tales datos puede suponer para los intereses, derechos y libertades fundamentales del interesado. Por tanto, el Convenio modernizado permite, en su artículo 11 ("*Exceptions and restrictions*"), excepciones al tratamiento de datos cuando tal excepción esté prevista por la ley, respete la esencia de los derechos y libertades fundamentales y "constituya una medida necesaria y proporcionada en una sociedad democrática para la protección de la seguridad nacional, la defensa, la seguridad pública, los intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial o la prevención, investigación y enjuiciamiento de los delitos penales y la ejecución de sanciones penales, y otros objetivos esenciales de interés público".

177. En definitiva, aunque el Convenio de Estrasburgo se elaboró y entró en vigor antes del surgimiento de Internet y de otras formas de tecnología de las comunicaciones, el hecho de que sus disposiciones estén formuladas en términos tecnológicamente neutros significa que las normas que establece siguen siendo pertinentes y de interés actual. La influencia del Convenio n. 108 es indudable en el campo concreto de la protección de datos personales tratados en el marco de la prevención y represión penal[297].

[296] MODERNISED CONVENTION for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018). Disponible en Internet: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf [consulta: 19 de septiembre de 2018].

[297] La mayor parte de las normativas dictadas en «*el antiguo tercer pilar comunitario señalan al Convenio n. 108, como la norma aplicable para determinar el nivel mínimo a garantizar por parte de los Estados miembros para el tratamiento de los datos personales. Entre ellos, destacamos: la Decisión Marco 2006/960/JAI del*

178. El ámbito de aplicación del Convenio[298], como estándar universal así como su "carácter abierto"[299], podrían ser "un presupuesto para promover la protección de los datos a nivel mundial"[300]. De hecho, la adhesión al Convenio n. 108 por parte de Estados que no forman parte del Consejo de Europa supone que puedan convertirse en miembros de pleno derecho del Comité y beneficiarse del foro que constituye dicho órgano para intercambiar conocimientos, buenas prácticas e información. Además, el país que se adhiere obtiene una garantía para que pueda tener lugar la transferencia recíproca de datos personales, cuestión esta de extrema importancia y a valorar por países como los EE.UU.; en particular, al haberse antes invalidado por el Tribunal de Justicia de la Unión Europea la Decisión de la Comisión sobre el Acuerdo de "Puerto Seguro", que permitía a las empresas estadounidenses adheridas al Acuerdo realizar la transferencia internacional de datos de carácter personal con Europa, así como el posterior y muy criticado nuevo Acuerdo "Puerto Seguro"[301].

179. En fin, si bien se hace referencia al tratamiento automatizado de los datos, de hecho, el Convenio ha establecido una regulación común, básica y fundamental para el fenómeno del tratamiento de datos personales, teniendo en cuenta su carácter transversal a múltiples ámbitos de la experiencia humana. Por lo tanto, el Convenio de Estrasburgo ha sido y sigue siendo un texto jurídico de referencia en este ámbito: impone a los Estados conceder garantías "mínimas"[302] pero irrenunciables. Ahora bien, corresponde a ellos concretar y precisar los principios básicos establecidos en este instrumento, que constituye patrimonio jurídico común de todas las partes contrayentes; su propia formulación, amplia y elástica permite adaptarse a los cambios impulsados principalmente desarrollos tecnológicos. Destaca asimismo la importancia de una interpretación evolutiva de los principios del Convenio en armonía con las exigencias impuestas por el artículo 8 del CEDH.

Consejo de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea; la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza; la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal». Alejandro Luis GACITÚA ESPÓSITO (2014: 140).

[298] Hasta el momento, ha sido ratificado por 53 Estados. La lista de los Estados parte del Convenio n. 108 y del Protocolo de 2001 pueden consultarse en la siguiente dirección: http://conventions.coe.int/Treaty/Commun/Cherchesig.asp?NT=108&cl=eng [consulta: 21 de septiembre de 2018].

[299] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 17).

[300] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 17).

[301] Dicho de otro modo, como veremos, el asunto *Schrems contra Facebook* planteado delante del TJUE ha dejado en una situación muy delicada a las empresas europeas que transfieren datos a Estados Unidos. Sería un buen momento para plantearse por parte de estos últimos su incorporación a dicho instrumento. El espinoso asunto será analizado en detalle en la sección sobre la actividad del Tribunal de Justicia de la Unión Europea.

[302] Alfonso ORTEGA GIMÉNEZ (2015).

En este contexto, las disciplinas del Convenio n. 108 son de importancia esencial, al inspirar los estándares del TEDH así como la jurisprudencia del Tribunal de Justicia de la Unión Europea.

CAPÍTULO II

EQUILIBRAR LA PRIVACIDAD Y LA SEGURIDAD NACIONAL EN LOS SISTEMAS CONSTITUCIONALES DE LA UNIÓN EUROPEA HASTA LA NUEVA REFORMA DE LA PROTECCIÓN DE DATOS

1. Contexto y antecedentes de la normativa europea de protección de datos

1. La disciplina de la privacidad aplicable en Europa nos ayuda a aclarar algunas distinciones conceptuales necesarias, en parte ya anticipadas. Tenemos que acudir, esencialmente, «*por una parte, al proceso evolutivo que ha sufrido este derecho fundamental, y por otra, hacer mención de las diversas fuentes de las cuales proviene su regulación, tanto supranacionales provenientes de los convenios del Consejo de Europa, como de las normas emanadas de las diversas fases del proceso de consolidación de la Unión Europea*»[303]. Es por ello por lo que esta parte recoge los más importantes instrumentos legislativos en la materia, hasta la nueva reforma de la protección de datos, relacionados con el difícil equilibrio entre privacidad y seguridad pública, en el marco de la Unión Europea. Este marco regulatorio ha permitido a Europa convertirse en uno de los escenarios institucionales, políticos y geográficos en el que el derecho fundamental a la "*privacy*" ha tenido mayor impulso. Este desarrollo empezó a partir de los años sesenta[304], hasta la consagración definitiva del derecho a la privacidad, o más bien el derecho a la protección de los datos personales, como derecho fundamental autónomo determinado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000.

[303] Alejandro Luis GACITÚA ESPÓSITO (2014: 124). A diferencia del Consejo de Europa, que nació para proteger los derechos fundamentales de los ciudadanos en un ámbito de cooperación entre Estados, la Unión Europea surgió con el ánimo de la integración económica de sus países miembros, bajo un paraguas de orden supraestatal, en el que todos ellos renunciaban a parte de su soberanía en favor de la Comunidad.

[304] La protección a los derechos fundamentales en el Derecho de la Unión (Derecho Comunitario hasta el Tratado de Lisboa de 2009) no se consideró materia necesaria en los inicios de la Comunidad Europea, y ello porque todos los miembros de la Comunidad lo eran a su vez del Consejo de Europa y habían suscrito previamente el CEDH de 1950. Entendían pues (tras varios debates en los que se planteó la posibilidad de elaborar un catálogo de derechos fundamentales) que dicha materia estaba suficientemente cubierta. Así se reconoce en 1977 en la Declaración Común del Parlamento Europeo, del Consejo y de la Comisión, en la que «(…) *subrayan la importancia primordial que atribuyen al respecto de los derechos fundamentales que resultan en particular de las constituciones de los Estados miembros, así como de la Convención Europea de Protección de los Derechos del Hombre y de las Libertades Fundamentales.* (…) *En el ejercicio de sus competencias y en cumplimiento de los objetivos de las Comunidades Europeas, respetarán y seguirán respetando tales derechos*». En DECLARACIÓN COMÚN DEL PARLAMENTO EUROPEO, DEL CONSEJO Y DE LA COMISIÓN, *Diario Oficial*, n. C 103 de 27/04/1977, págs. 0001 – 0002. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31977Y0427(01) [consulta: 16 de enero de 2016].

2. En la UE, el derecho a la privacidad está garantizado y se rige tanto por los Tratados como por la legislación secundaria. Tras la aprobación del Tratado de Lisboa, el artículo 16 del TFUE rige el derecho fundamental al tratamiento de datos personales, estableciendo los procedimientos para la protección normativa de esta esfera. El artículo 16 establece las competencias de la UE para proteger los datos personales, indicando que el Parlamento Europeo y el Consejo, actuando de conformidad con el procedimiento legislativo ordinario, aprobarán normas capaces de salvaguardar a los ciudadanos del uso indebido de sus datos personales por parte de las instituciones de la UE y los Estados miembros al realizar actividades que entran dentro del ámbito de aplicación del Derecho de la Unión.

3. Este artículo opera en conjunto con todas las competencias europeas, especialmente las disposiciones del mercado interno, ya que la creación de este mercado, junto con la llegada de la era digital, ha dado como resultado la transmisión constante de información y datos digitales. Al establecer la base legal para el procesamiento de datos europeo, al reconocer una libertad fundamental, el artículo 16 aclara que cuando exista un conflicto entre la protección de la privacidad y la libre circulación de datos personales hace imposible encontrar un equilibrio, el primero debe prevalecer.

4. La evolución y adaptación de este derecho, sobre todo, después del Tratado Lisboa que ha reconocido al mismo derecho valor legal completo, encuentra un reconocimiento formal a nivel europeo no sólo en el proceso constitucional del derecho a la protección de los datos personales, como veremos más adelante, sino en algunas constituciones nacionales y en la inspiración de las intervenciones por parte de los Tribunales europeos (TEDH y TJUE), así como también el camino de su propia autonomía con respecto a otras situaciones jurídicas subjetivas, en particular el derecho a la privacidad. De hecho, recordamos que el derecho a la privacidad es el derecho de toda persona a ver protegido su vida privada frente a la injerencia de las autoridades públicas y de la curiosidad de los demás.

5. Además, la protección "constitucional" del derecho a la privacidad y la protección de datos está expresamente garantizada para cada individuo por los artículos 7 y 8 de la CDFUE. El artículo 7 de la Carta establece específicamente la disposición general de que «*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*». El artículo 8 de la misma protege el derecho a la protección de los datos personales, y establece que tales datos deben tratarse de manera «*leal, para fines concretos y sobre la base del consentimiento*» del interesado o de cualquier otra base

legítima establecida por la ley, así como que cada persona tiene el derecho de acceso a los datos recogidos sobre ella, y el derecho a que se rectifique. La protección de los datos personales es en principio independiente del derecho garantizado en el artículo 7, ya que regula la protección del individuo en relación con los desafíos de la era digital, que requieren adoptar los principios establecidos en el Preámbulo de la Carta, según el cual debe garantizarse la protección de los derechos europeos a la luz de los cambios en la sociedad, el progreso social y los avances científicos y tecnológicos.

6. Los actos legislativos especiales en realidad garantizaban este derecho incluso antes de que se adoptaran estas normas en el Tratado. Durante muchos años[305], la herramienta principal de la antigua estructura de pilares -aunque junto con otros actos específicos[306]- para dicha protección fue la Directiva de protección de datos de la UE (95/46/CE), que exigía a los Estados miembros proteger los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho a la privacidad, con respecto al tratamiento de datos personales, así como instrumentos pertenecientes al antiguo tercer pilar, como la Decisión Marco del Consejo, de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

7. En este contexto, la Directiva 95/46/CE y la Decisión Marco del Consejo de 2008 fueron reemplazadas recientemente por el llamado "paquete de protección de datos personales", que consiste en el Reglamento (UE) 2016/679, que introduce reglas generales uniformes en el Derecho de la Unión y la Directiva (UE) 2016/680, y que rige la protección de datos en relación con la cooperación policial y judicial al prevenir, investigar, detectar o enjuiciar delitos. Estas disposiciones ahora brindan una nueva y generalizada protección de la privacidad, adoptando las indicaciones emitidas por el TJUE y el Grupo de Trabajo del Artículo 29 en la interpretación del Derecho de la Unión.

[305] En particular en Europa, con la introducción de las primeras herramientas tecnológicas y de la creciente informatización de las relaciones autoridades públicas-ciudadanos, el legislador europeo ha puesto el problema de la necesidad de una específica tutela teniendo en cuenta la relación entre la confidencialidad y el uso de la computadora. La relevancia de la protección de datos es principalmente el resultado de la necesidad de armonizar las diferentes disciplinas estatales que se fortalecieron desde principios de los años setenta. De ahí surgió, con retraso respecto de muchos órdenes estatales europeos, la necesidad de adoptar la Directiva 95/46/CE, relativa al tratamiento de los datos personales y de su libertad de movimiento. Para más información sobre la evolución de la normativa en protección de datos, véase entre todos, Concepción CONDE ORTIZ (2005), *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Cádiz, Dykinson, págs. 116; Lucrezio REBOLLO DELGADO y María Mercedes SERRANO PÉREZ (2014), *Manual de protección de datos*, Madrid, Dikynson, págs. 354.

[306] *Vid*. *infra*.

8. En fin, en este Capítulo revisaremos la normativa general que estaba vigente en Europa en tema de protección de datos personales hasta la reforma de la protección de datos de 2016 en la Unión (de aplicación a partir de mayo de 2018). Comenzaremos este estudio con el Tratado de Lisboa, «*por la transcendencia que tiene en el cambio de la arquitectura institucional y normativa de la Unión, y que en el ámbito específico del derecho fundamental a la protección de datos se traduce en una nueva base jurídica*»[307]. A continuación analizaremos los principales actos legislativos sobre la materia y su vinculación con el tratamiento de datos personales en el ámbito policial.

2. La constitucionalización de la protección de datos personales en el Tratado de Lisboa

9. Desde la entrada en vigor del Tratado de Lisboa[308], el 1 de diciembre de 2009, la UE tiene una específica y explícita base jurídica para la protección de datos[309]. El Tratado constitutivo de la Comunidad Europea (en adelante, TCE) pasa a denominarse Tratado de Funcionamiento de la Unión Europea (TFUE) y el término «Comunidad» se sustituye por «Unión» en todo el texto. La Unión ocupa el lugar de la Comunidad y la sucede desde el

[307] Alejandro Luis GACITÚA ESPÓSITO (2014: 146).

[308] TRATADO DE LISBOA POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA Y EL TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA, *Diario Oficial de la Unión Europea*, C 306 de 17 de diciembre de 2007.

[309] Sobre el Tratado de Lisboa *vid*., entre muchos, Juan José ÁLVAREZ RUBIO (2006), «Libertad, seguridad y justicia en la nueva Europa», en Susana DEL RÍO VILLAR (coord.), *Europa: el Estado de la Unión*, Navarra, Editorial Aranzadi, págs. 119-138. ISBN 84-8355-029-6; Paz ANDRÉS SÁENZ DE SANTA MARÍA (2007), «El Tratado de Lisboa: Comienza una nueva etapa para Europa», en *Diario La Ley*, núm. 6851. ISSN 1989-6913; Gurutz JÁUREGUI BERECIARTU y Juan Ignacio UGARTEMENDÍA ECEIZABARRENA (2007), «Europa en el lecho de Procusto: de la Constitución Europea al Tratado de Lisboa», en *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkarian*, núm. 79, págs. 105-126. ISSN 0211-9560; Francisco ALDECOA LUZÁRRAGA y Mercedes GUINEA LLORENTE (2008), «El rescate sustancial de la Constitución Europea a través del Tratado de Lisboa: la salida del laberinto», en *Documento de Trabajo*, Real Instituto Elcano, núm. 9, págs. 32; Francisco BALAGUER CALLEJÓN (2008), «El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea», en *Revista Española de Derecho Constitucional*, año 28, núm. 83, págs. 57-92. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2702876 [consulta: 29 de junio de 2017]; Alberto LUCARELLI e Andrea PATRONI GRIFFI (a cura di) (2009), *Dal Trattato costituzionale al Trattato di Lisbona: nuovi studi sulla Costituzione europea*, Napoli, Edizioni Scientifiche Italiane, págs. 526; José MARTÍN Y PÉREZ DE NANCLARES y Mariola URREA CORRES (2010), *Tratado de Lisboa. Textos consolidados del tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea*, 2ª edición, Madrid, Marcial Pons y Real Instituto Elcano, págs. 395; Francisco ALDECOA LUZÁRRAGA y Mercedes GUINEA LLORENTE (2010), *La Europa que viene: el Tratado de Lisboa*, Madrid, Editorial Marcial Pons, págs. 411; Antonio D'ATENA (2010), «La Constitución oculta de Europa (antes y después de Lisboa)», en *Revista de Derecho Constitucional Europeo*, año 7, núm. 13. Disponible en Internet: http://www.ugr.es/~redce/REDCE13/articulos/01DAtena.htm [consulta: 29 de junio de 2017]; Lucía MILLÁN MORO (2010), «El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa», en *Revista de Derecho Comunitario Europeo*, núm. 36, págs. 401-438. Disponible en Internet: http://www.cepc.gob.es/gl/publicaci%C3%B3ns/revistas/revistas-electronicas?IDR=4&IDN=1260&IDA=27881 [consulta: 30 de junio de 2017].

punto de vista jurídico (artículo 1 del TUE). La promulgación del Tratado de Lisboa supuso la consolidación del derecho fundamental a la protección de datos como un derecho independiente y autónomo, si bien no está exenta de críticas por su contenido insuficiente[310].

10. Dejando de lado los importantes cambios que introduce el Tratado[311], nos centramos en aquellos que interesan a la investigación.

11. El Tratado de Lisboa crea, por primera vez, una nueva base jurídica para la protección de datos personales en el Espacio de Libertad, Seguridad y Justicia[312] (ELSJ), que se utiliza tanto para la armonización de las leyes del mercado interior como para la cooperación judicial civil y penal (*ex* tercer pilar)[313]. En concreto, el equivalente artículo 3, apartado 2 de la versión consolidada del Tratado de la Unión Europea (en adelante, TUE), establece que: «*la Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia*».

[310] En este sentido Carlos RUIZ MIGUEL (2003), «El Derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Análisis crítico», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, págs. 7-43.

[311] El Tratado de Lisboa no transfiere nuevas competencias exclusivas a la Unión. No obstante, al fomentar la participación y la protección de los ciudadanos, crea un nuevo orden institucional y modifica los procesos de toma de decisiones en aras de una mayor eficacia y transparencia, en respuesta a la supresión de la antigua estructura de pilares, cambia la forma en que la Unión ejerce sus competencias ya existentes, a las que se suman algunas competencias nuevas (compartidas), mayores competencias para el TJUE y un nuevo cometido para los Parlamentos nacionales. De este modo, garantiza asimismo un mayor nivel de control parlamentario y responsabilidad democrática. *Vid*. Petr NOVAK y Rosa RAFFAELLI (2017), «El Tratado de Lisboa», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo, págs. 5. Disponible en Internet: http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.1.5.pdf [consulta: 30 de junio de 2017].

[312] El Título V del TFUE (artículos 67 a 89) está dedicado al ELSJ. Este Título incluye los siguientes capítulos distintos dedicados a: 1) Disposiciones generales; 2) Políticas sobre controles en las fronteras, asilo e inmigración; 3) Cooperación judicial en materia civil; 4) Cooperación judicial en materia penal; 5) Cooperación policial. *Vid*. *amplius*, Dino Guido RINOLDI (2010), «Lo spazio di libertà, sicurezza e giustizia», en Ugo DRAETTA, Nicoletta PARISI (eds.), *Elementi di diritto dell'Unione europea. Parte speciale. Il diritto sostanziale*, Giuffrè Editore, págs. 1- 94; y, del mismo autor (2012), *Lo spazio di libertà, sicurezza e giustizia nel diritto dell'integrazione europea. I. Principi generali e aspetti penalistici*, Napoli, Editoriale scientifica, págs. 354. 978-88-6342-246-7; y también Víctor Luis GUTIÉRREZ DEL CASTILLO y Manuel LÓPEZ JARA (2017), *El desarrollo y consolidación del Espacio de Libertad, Seguridad y Justicia de la UE. La implementación del Programa de Estocolmo*, Madrid, Editorial Tecnos, págs. 301. ISBN: 978-84-309-7070-4.

[313] Sarah SY (2017a), «Un espacio de libertad, seguridad y justicia: aspectos generales», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.12.1.html [consulta: 01 de julio de 2017].

12. Este artículo, que tiene por objeto definir los principales objetivos perseguidos por la UE[314], concede mayor importancia a la creación de un ELSJ que el anterior Tratado de Niza[315], porque ahora este objetivo se menciona incluso antes de la creación de un mercado interior[316]. También, como expresión de la mayor elasticidad en el proceso de construcción europea que supone el Tratado de Lisboa, se prevé la posibilidad de algunas excepciones en el cumplimiento de las disposiciones europeas[317]. Nos referimos al caso de Reino Unido e Irlanda que participan sólo en la adopción y aplicación de medidas específicas a raíz de una decisión de participación ("*opt-in*")[318].

[314] Con el fin de favorecer un ELSJ, no hace falta olvidar el papel que los Parlamentos nacionales tienen en tal sentido, los cuales contribuirán activamente al buen funcionamiento de la Unión, «*participarán, en el marco del espacio de libertad, seguridad y justicia, en los mecanismos de evaluación de la aplicación de las políticas de la Unión en dicho espacio, de conformidad con el artículo 70 del Tratado de Funcionamiento de la Unión Europea, y estarán asociados al control político de Europol y a la evaluación de las actividades de Eurojust, de conformidad con los artículos 88 y 85 de dicho Tratado*» (artículo 12, letra c), del TUE). Véase también artículos 85 y 88 del TFUE, juntamente con artículo 9 del Protocolo n. 1 y artículo 51 del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (*vid*. Capítulo III de esta investigación). En particular, sobre cómo los Parlamentos nacionales se han adaptado a sus nuevas funciones y cómo el nuevo sistema ha tenido un impacto sobre las relaciones entre los cuerpos legislativos de la UE y los Parlamentos nacionales, *vid*. Anna JONSSON CORNELL, Marco GOLDONI (eds.) (2017), *National and Regional Parliaments in the EU-Legislative Procedure Post-Lisbon. The Impact of the Early Warning Mechanism*, Hart Publishing, págs. 384.

[315] El Tratado de Niza refuerza la legitimación del Parlamento Europeo en el sistema jurisdiccional comunitario, facultándolo para interponer el recurso de anulación (artículo 230 del TCE), y de solicitar dictámenes al TJUE sobre la compatibilidad con las disposiciones del Tratado de los acuerdos internacionales celebrados por la Comunidad (artículo 300, apartado 6, del TCE). Tales atribuciones conferidas al Parlamento pueden considerarse, a nuestro juicio, una de las modificaciones más positivas en cuanto a la crítica que pudieran merecer las novedades introducidas por el Tratado de Niza. Tal afirmación se confirma, por ejemplo, en las nuevas funciones como la interposición del recurso de anulación en los asuntos acumulados C-317/04 y C-318/04 por el que el Parlamento Europeo solicitaba que se anulase la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos y la anulación de la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombre de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*vid*. Capítulo IV de esta investigación). José MARTÍN Y PÉREZ DE NANCLARES (2007), «La posición del Parlamento Europeo en el espacio de libertad, seguridad y justicia», en Esther BARBÉ, Anna HERRANZ SURRALLÉS (eds.), *Política exterior y Parlamento Europeo: hacia el equilibrio entre eficacia y democracia*, págs. 67-83. ISBN 978-92-823-2183-6.

[316] *Vid*. Gloria MARCHETTI (2012), «I recenti passi avanti compiuti dall'Unione europea nella direzione di un'armonizzazione dei sistemi penali. Aspetti positivi, aspetti problematici e prospettive di riforma», en *Research Paper Centro Studi sul Federalismo*, págs. 4 y ss.

[317] Como algunos autores han llamado «*La Europa a la carta, o de varias velocidades*». *Vid*. Sergio CARRERA y Florian GEYER (2008), «El Tratado de Lisboa y un Espacio de Libertad, Seguridad y Justicia: Excepcionalismo y Fragmentación en la Unión Europea», en *Revista de Derecho Comunitario Europeo*, núm. 29, pág. 134. ISSN 1138-4026. Disponible en Internet: https://recyt.fecyt.es//index.php/RDCE/article/view/46494 [consulta: 13 de marzo de 2016].

[318] Reino Unido e Irlanda, no aplican las disposiciones sobre la cooperación judicial y policial en materia penal, tal como lo establece un Protocolo adicional al Tratado de Lisboa. Protocolo (n. 21) sobre la posición del Reino Unido y de Irlanda respecto del ELSJ. Dinamarca no participa en la adopción por el Consejo de medidas propuestas en virtud del Título V del TFUE. Protocolo (n. 22) sobre la posición de Dinamarca. *Vid*. VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA - Protocolos - Anexos - Declaraciones anejas al Acta Final

13. Más específicamente a lo que nos interesa, la unificación de los tres pilares tradicionales en un único marco jurídico europeo, inspirado en reglas y principios comunes y la aplicación de normas y principios idénticos, es uno de los aspectos más importantes del Tratado de Lisboa[319]. La consagración del derecho a la protección de los datos personales como un derecho individual de la persona, está presente en dos disposiciones del Tratado de Lisboa que se compone, como es sabido, del TFUE y el TUE.

14. De acuerdo con lo dispuesto en el artículo 6 del TUE, la Unión identifica como su núcleo fundamental, de hecho, los "principios de libertad, democracia, respeto de los derechos humanos y el Estado de Derecho": «*1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones. 2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados. 3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales*». El artículo en comentario reconoce por primera vez la existencia de estos derechos (libertad, democracia y los derechos y libertades fundamentales) señalándolos como principios generales del

de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa firmado el 13 de diciembre de 2007 - Tablas de correspondencias, *Diario Oficial de la Unión Europea*, núm. C 326 de 26/10/2012, págs. 0001–0390. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012M%2FTXT [consulta: 13 de junio de 2015].

[319] Antes de la entrada en vigor del Tratado de Lisboa, la legislación relativa a la protección de datos en el ELSJ estaba repartida entre el primer pilar (protección de datos con fines privados y comerciales, sometida al método comunitario) y el tercer pilar (protección de datos con fines de aplicación de la ley, con toma de decisiones a escala intergubernamental). En consecuencia, el proceso decisorio se regía por dos normativas diferentes. La estructura de pilares desapareció con el Tratado de Lisboa, que aporta una base más sólida para desarrollar un sistema de protección de datos más claro y eficaz, al tiempo que prevé nuevas competencias para el Parlamento Europeo, que se convierte en colegislador.

derecho, y conectándolos con el CEDH, así como con las «*tradiciones constitucionales comunes de los Estados miembros*»[320].

15. En particular, la Carta de los Derechos Fundamentales de la UE y de los derechos mencionados en ella, en virtud del artículo 6, apartado 1, del TUE, han asumido rango de derecho primario en las fuentes europeas, confiriéndole así el mismo valor jurídico que los Tratados[321] (*vid*. *infra*). En el mismo artículo, apartado 2, se consagra que la Unión se adherirá al CEDH. Siguiendo, los derechos fundamentales pronunciados explícitamente y las «*tradiciones constitucionales comunes de los Estados miembros*», pasan a constituir «*principios generales*»[322] del Derecho de la Unión.

16. El artículo 6 del TUE se relaciona con la «*protección de datos en el ámbito de la cooperación judicial y policial en materia penal, ya que es aplicable a la cooperación judicial y policial. Por tanto, para la adecuada interpretación de las normas sobre protección de datos en lo vinculado a la prevención y represión penal*», y consecuentemente a la seguridad pública, «*debemos tener presente tanto el CEDH como las tradiciones constitucionales comunes de los Estados miembros*»[323].

[320] Así Juan Fernando LÓPEZ AGUILAR (2017), «La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU», en *UNED. Teoría y Realidad Constitucional*, núm. 39, pág. 557. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19165 [consulta: 01 de agosto de 2017].

[321] Sabemos que el Derecho de la UE consiste en los Tratados y en el derecho derivado de la UE. Los Tratados, es decir el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), también conocidos como "derecho primario de la UE", han sido aprobados por todos los Estados miembros de la UE. Los reglamentos, directivas y decisiones de la UE, adoptados por las instituciones de la UE que se han dado esta autoridad en virtud de los tratados, se refieren a menudo como derecho de la UE. *Vid*. Giuseppe TESAURO (2012), *Diritto dell'Unione europea*, 7ª ed., Padova, Cedam, págs. 960. ISBN: 978-88-13-31534-4. En la doctrina en general se observa que la Carta de los Derechos Fundamentales de la Unión Europea no otorga a las instituciones de la UE facultades para intervenir directamente en el campo de los derechos humanos, este límite no existe en relación con el derecho a la protección de datos personales. Stella COGLIEVINA (2013), *Diritto antidiscriminatorio e religione. Uguaglianza, diversità e libertà religiosa in Italia, Francia e Regno Unito*, Libellula Edizioni, págs. 40-41.

[322] *Vid*. Juan Fernando LÓPEZ AGUILAR (2017: 557-558).

[323] Alejandro Luis GACITÚA ESPÓSITO (2014: 149). En particular, «*si bien se pretende mejorar la coordinación y la eficacia de las políticas de seguridad, de lucha contra la delincuencia organizada, contra el latente terrorismo global, o para hacer frente a los flujos migratorios,* (…) *también se refuerza la exigencia del respeto a los derechos fundamentales en esa labor, auténtico caballo de batalla de los tiempos actuales. En la misma línea, el art. 67.1 del texto consolidado del TFUE, afirma que "La Unión constituye un espacio de libertad, seguridad y justicia dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicas de los Estados miembros"*». En Joan Lluís PÉREZ FRANCESCH (2012), «El Tratado de Lisboa: cooperación policial y judicial entre la europeización y las reservas estatales», en Elías SAID HUNG (Editor), *Diálogos y desafíos euro-latinoamericanos: ensayos sobre cooperación, derecho, educación y comunicación*, Barranquilla, Editorial Universidad del Norte, págs. 81-82.

17. A partir del 1 de diciembre de 2009, fecha de la entrada en vigor del Tratado de Lisboa, todas «*las instituciones, órganos y organismos de la Unión*», además de «*los Estados miembros*», ahora están obligados a garantizar el respeto de los derechos fundamentales en el ejercicio de las «*competencias*» atribuidas por los Tratados[324]. En este contexto, un papel importante es el desarrollado por el Tribunal de Justicia[325], previendo además por la CDFUE que todas personas cuyos derechos y libertades que alegan haber sido violados tienen derecho a un recurso efectivo ante los jueces también de la UE[326]. En particular, aunque ya sucedía antes de la reforma de Lisboa, este último ha asegurado una protección reforzada de los derechos fundamentales de los ciudadanos europeos contra las iniciativas de las instituciones europeas y de los Estados miembros.

18. La nueva arquitectura de la UE, cada vez con más atención a la protección de los derechos de ciudadanía, ha asignado al Tribunal de Justicia el papel de juez de los derechos fundamentales[327], que se consolidará y definirá sin duda mejor como consecuencia de la adhesión de la Unión al CEDH en virtud del artículo 6, apartado 2 del TUE[328], ahora en fase de negociación (sobre el papel del TJUE, véanse Capítulo IV).

---

[324] Artículo 51 (Ámbito de aplicación) de la CDFUE: «*1. Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión. 2. La presente Carta no amplía el ámbito de aplicación del Derecho de la Unión más allá de las competencias de la Unión, ni crea ninguna competencia o misión nuevas para la Unión, ni modifica las competencias y misiones definidas en los Tratados*».

[325] Sergio CARRERA, Marie DE SOMER and Bilyana PETKOVA (2012), «The Court of Justice of the European Union as a Fundamental Rights Tribunal Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice», en *CEPS Paper in Liberty and Security in Europe*, núm. 49, págs. 29. ISBN: 978-94-6138-222-1. Disponible en Internet: http://aei.pitt.edu/36443/1/No_49_Carrera_et_al__ECJ_as_Fundamental_Rights_Tribunal2-2.pdf [consulta: 18 de mayo de 2015].

[326] Artículo 47 (Derecho a la tutela judicial efectiva y a un juez imparcial) de la CDFUE: «*Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la Ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia*».

[327] Esta nueva función de los jueces de Luxemburgo, que es y será ejercida principalmente en los juicios contemplados en los artículos 256, 263 y 267 del TFUE, hará que se requiera aún más que antes el equilibrio de los diversos derechos involucrados con el fin de establecer, caso por caso, la prevalencia de uno sobre el otro.

[328] Sobre este importante asunto, el TJUE se ha pronunciado en contra de la adhesión de la Unión en bloque al CEDH. *Vid*. TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA - Comunicado de prensa núm. 180/14, El Tribunal de Justicia se pronuncia sobre el Proyecto de acuerdo de adhesión de la Unión Europea al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales e identifica problemas de compatibilidad con el Derecho de la Unión, dictamen 2/13, Luxemburgo, 18 de diciembre de 2014. Disponible en Internet: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140180es.pdf [consulta: 08 de enero de 2016].

2.1. El Tratado de Lisboa: ¿nuevos horizontes para la protección de datos personales en la Unión Europea?

19. La consolidación del ELSJ y los cambios introducidos por el Tratado de Lisboa[329], han cambiado el marco institucional dentro del cual el derecho a la protección de los datos personales opera en la Unión Europea, extendiéndola más allá de los estrechos confines del mercado interior. La adopción del Tratado es "un hito en el desarrollo de la normativa de protección de datos", no sólo para elevar, como notaremos, la CDFUE al Estado de un documento jurídico vinculante a nivel de derecho primario, sino también para proporcionar el derecho a la protección de datos personales[330]. Esto queda claro a partir del artículo 16 del TFUE (antiguo artículo 286 del TCE)[331], en virtud de la parte del Tratado dedicada a los principios generales de la UE; disposición que encuentra aplicación general en la competencia de la Unión.

20. El artículo 16 crea una nueva base jurídica independiente que atribuye al legislador europeo competencia concurrente[332] con los Estados para adoptar, según el procedimiento ordinario, las normas relativas a la protección de las personas con respecto al tratamiento de sus datos personales, así como las relativas a la libre circulación de estos datos. Éste es un avance importante porque las normas de protección de datos de la UE - en particular, la Directiva de protección de datos de 1995 - se basaron inicialmente en el fundamento jurídico del mercado interior y en la necesidad de aproximar las legislaciones nacionales para evitar

[329] Paul DE HERT, Vagelis PAPAKONSTANTINOU and Cornelia RIEHLE (2008), «Data protection in the Third Pillar: Cautious pessimism», en Martin MAIK, (ed.), *Crime Rights and the EU: The Future of the Police and Judicial Cooperation*, London, Justice, pág. 122. Disponible en Internet: http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf [consulta: 19 de mayo de 2015].

[330] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[331] El artículo 286 del TCE, introducido por el Tratado de Ámsterdam (*vid*. *infra*), ha establecido explícitamente la obligación de cumplir con las normas de protección de datos personales por parte de las instituciones y organismos europeos. Este artículo demandaba, también, al Consejo y al Parlamento la creación de un órgano de control independiente. Unos años más tarde, en 2001, y como desarrollo del mandato contenido en el TCE, y también en la Directiva 95/46/CE sobre protección de datos personales, se aprueba el Reglamento 45/2001 sobre protección de datos personales por parte de las instituciones y órganos comunitarios, que crea una administración independiente encargada de la protección de los datos personales, el "Supervisor Europeo de Protección de Datos", con lo cual se dota a la protección de datos personales de una garantía específica y reforzada. Mónica ARENAS RAMIRO (2008: 125).

[332] *Vid*. Sandro DI MINCO (2012), «Commento all'art. 16 del TFUE», en Carlo CURTI GIALDINO (dir.), *Codice dell'Unione Europea Operativo. TUE e TFUE commentati articolo per articolo*, Napoli, Edizioni Giuridiche Simone, págs. 2560; Bernardo CORTESE (2013), «La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona», en *Il Diritto dell'Unione Europea*, núm. 2, págs. 313-335. Sobre el tema de la asignación de las competencias en consecuencia de la reforma del Tratado de Lisboa, vid. Lucia Serena ROSSI (2012), «Does the Lisbon Treaty Provide a Clearer Separation of Competences between EU and Member States?», en Andrea BIONDI, Piet EECKHOUT, and Stefanie RIPLEY (eds.), *EU Law After Lisbon*, New York, págs. 85-106; Albrecht WEBER (2012), «The Distribution of Competences Between the Union and the Member States», en Hermann-Josef BLANKE, Stelio MANGIAMELI (eds.), *The European Union After Lisbon. Constitutional Basis, Economic Order and External Action*, Springer Berlin Heidelberg, págs. 311-322.

la libre circulación de datos dentro de la UE[333]. La cuestión de la protección de datos personales no está incluida en las listas mencionadas en los artículos 3 y 4 del TFUE[334]. En términos formales, la lista de materias exclusivas del artículo 3 se considera obligatoria, mientras que las del artículo 4 es, obviamente, una lista no exhaustiva, dada la naturaleza residual de las competencias concurrentes.

21. La protección de datos, además de ser un derecho fundamental reconocido en todos los aspectos, también se convierte, con el artículo 16 del TFUE, en la base jurídica independiente para la acción de la UE en la materia. La protección de datos en la UE no es, en otras palabras, dejada a la sola acción de control del Tribunal de Justicia, sino también a la del legislador de la UE, a través de la construcción de un marco moderno e integral de plena protección y adecuada a las nuevas exigencias del sistema internacional, que abarca todos los asuntos de competencia de la UE, incluida la cooperación policial y judicial en materia penal: «*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se*

[333] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[334] Artículo 3 del TFUE: «*1. La Unión dispondrá de competencia exclusiva en los ámbitos siguientes: a) la unión aduanera; b) el establecimiento de las normas sobre competencia necesarias para el funcionamiento del mercado interior; c) la política monetaria de los Estados miembros cuya moneda es el euro; d) la conservación de los recursos biológicos marinos dentro de la política pesquera común; e) la política comercial común. 2. La Unión dispondrá también de competencia exclusiva para la celebración de un acuerdo internacional cuando dicha celebración esté prevista en un acto legislativo de la Unión, cuando sea necesaria para permitirle ejercer su competencia interna o en la medida en que pueda afectar a normas comunes o alterar el alcance de las mismas*». Artículo 4 del TFUE: «1. *La Unión dispondrá de competencia compartida con los Estados miembros cuando los Tratados le atribuyan una competencia que no corresponda a los ámbitos mencionados en los artículos 3 y 6. 2. Las competencias compartidas entre la Unión y los Estados miembros se aplicarán a los siguientes ámbitos principales: a) el mercado interior; b) la política social, en los aspectos definidos en el presente Tratado; c) la cohesión económica, social y territorial; d) la agricultura y la pesca, con exclusión de la conservación de los recursos biológicos marinos; e) el medio ambiente; f) la protección de los consumidores; g) los transportes; h) las redes transeuropeas; i) la energía; j) el espacio de libertad, seguridad y justicia; k) los asuntos comunes de seguridad en materia de salud pública, en los aspectos definidos en el presente Tratado. 3. En los ámbitos de la investigación, el desarrollo tecnológico y el espacio, la Unión dispondrá de competencia para llevar a cabo acciones, en particular destinadas a definir y realizar programas, sin que el ejercicio de esta competencia pueda tener por efecto impedir a los Estados miembros ejercer la suya. 4. En los ámbitos de la cooperación para el desarrollo y de la ayuda humanitaria, la Unión dispondrá de competencia para llevar a cabo acciones y una política común, sin que el ejercicio de esta competencia pueda tener por efecto impedir a los Estados miembros ejercer la suya*».

entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea».

22. El artículo 16 del TFUE reviste una importancia crucial para la protección de los datos en muchas perspectivas y hay muchos aspectos que merecen destacarse en esta nueva disposición[335].

23. El artículo 16 del TFUE se divide en dos apartados: el primero establece el derecho de que se trate en los mismos términos usados en el artículo 8 de la CDFUE (*vid*. *infra*), y contribuya a fortalecer la dimensión constitucional tomada por el derecho a la protección de datos personales, que se une a un efecto directo para todos los individuos; mientras que el segundo proporciona la base jurídica para la adopción de normas de derecho secundario.

24. La *ratio* del apartado 1, artículo 16, es que el Tratado obliga directamente a todas las entidades públicas y privadas a respetar el derecho de que se trate[336]. Asimismo, la base jurídica es innovadora para la generalidad de su ámbito de aplicación: se pone como límite a la acción de los Estados e instituciones y también proporciona una intervención activa a las propias instituciones con el fin de garantizar la protección de las personas físicas respecto del tratamiento de datos de carácter personal. La acción de la Unión en esta materia puede llegar a prevalecer sobre la de los Estados miembros, no sólo en referencia a la libre circulación de datos, sino a la defensa del derecho en su conjunto. Aun así, es aspecto central y altamente innovador la afirmación del derecho a la protección de datos personales ya que la identificación como un objetivo de la Unión da lugar, en casos concretos de conflicto entre los dos intereses, a la prevalencia de la protección del derecho a la protección de los datos de carácter personal sobre la libre circulación de datos.

25. El segundo apartado, representa «*una nueva base jurídica introducida por el Tratado de Lisboa para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas*

[335] Bernardo CORTESE (2013: 316 y ss.).

[336] A diferencia de lo que ocurrió en el pasado con el artículo 286, apartado 1 del TCE: «(…) *que los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo*». TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA (Vigente hasta el 1 de diciembre de 2009).

en el ámbito de aplicación del Derecho de la Unión»[337]. También, se registra el control ejercido por las autoridades independientes del respeto de dichas normas en los Estados miembros. La supervisión independiente es un componente esencial de la normativa europea de protección de datos. Tanto la legislación de la UE como la del CdE consideran que la existencia de autoridades de supervisión independientes es indispensable para la protección efectiva de los derechos y libertades de las personas con respecto al procesamiento de sus datos personales. Como el procesamiento de datos ahora está siempre presente, y es cada vez más complejo de entender para las personas, estas autoridades son las vigilantes de la era digital. En la UE, la existencia de autoridades de supervisión independientes se considera uno de los elementos más esenciales del derecho a la protección de datos personales, consagrado en la legislación primaria de la UE. El artículo 8, apartado 3, de la CDFUE y el mismo artículo 16, apartado 2, del TFUE reconocen la protección de los datos personales como un derecho fundamental y afirman que el cumplimiento de las normas de protección de datos debe estar bajo control de una autoridad independiente[338].

26. El artículo 16 del TFUE, "introduce una base jurídica específica para la adopción de normas relativas a la protección de los datos personales, que también se aplica a la cooperación judicial en materia penal y la cooperación policial, y debido a la naturaleza específica del ámbito de la cooperación policial y judicial en materia penal, podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en este ámbito"[339]. En este sentido, para cumplir con lo establecido en el artículo 16, apartado 2, del TFUE, como veremos, «*la Comisión ha propuesto una serie de importantes reformas a las normas de la Unión Europea en materia de protección de los datos personales, que pretenden actualizar y modernizar los principios consagrados en la Directiva de 1995, para garantizar el derecho a la protección de los datos personales en el futuro*»[340]. El artículo concluye señalando que, en realidad, se adoptarán normas especiales para los datos personales tratados en el ámbito de la Política Exterior y de Seguridad Común de la Unión (en adelante, PESC).

[337] *Cfr*. Alejandro Luis GACITÚA ESPÓSITO (2014: 203); Alfonso SCIROCCO (2008), «The Lisbon Treaty and the Protection of Personal Data in the European Union», en *European Data Protection Review*, núm. 5; Ofelia TEJERINA RODRÍGUEZ (2014: 84 y ss.).
[338] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).
[339] Ofelia TEJERINA RODRÍGUEZ (2014: 85).
[340] Alejandro Luis GACITÚA ESPÓSITO (2014: 354).

27. Además, en las Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa, también encontramos alusiones a la protección de datos de carácter personal. Así, cuando se aprobó el Tratado de Lisboa se adoptó también la Declaración n. 20 relativa al artículo 16 del TFUE, que advierte que «*las normas sobre protección de datos de carácter personal* (…) *puedan tener una repercusión directa en la seguridad nacional, habrán de tenerse debidamente en cuenta las características específicas de la cuestión*»[341]. Se menciona que la legislación actualmente aplicable «*contiene excepciones específicas*» a este respecto[342]. En todo caso, sin perjuicio del artículo 39 del TUE, se le da al Consejo el poder de adoptar decisiones *ad hoc* con el fin de establecer «*normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros*» en la realización de actividades que entran en el ámbito de la PESC y sobre la libre circulación de estos datos[343].

28. Tal disposición constituye una excepción con respecto al procedimiento previsto por el segundo apartado del artículo 16 del TFUE y, como tal, será interpretada restrictivamente, dado el principio establecido por el artículo 40 del TUE (*ex* artículo 47 del TUE), apartado 1, según el cual la ejecución de la PESC no afecta «*a la aplicación de los procedimientos y al alcance respectivo de las atribuciones de las instituciones establecidos en los Tratados para el ejercicio de las competencias de la Unión mencionadas en los artículos 3 a 6 del Tratado de Funcionamiento de la Unión Europea*»[344].

---

[341] Declaración n. 20 relativa al artículo 16 del TFUE: «*La Conferencia declara que, siempre que las normas sobre protección de datos de carácter personal que hayan de adoptarse con arreglo al artículo 16 puedan tener una repercusión directa en la seguridad nacional, habrán de tenerse debidamente en cuenta las características específicas de la cuestión. Recuerda que la legislación actualmente aplicable (véase, en particular, la Directiva 95/46/CE) contiene excepciones específicas a este respecto*». En DECLARACIONES ANEJAS AL ACTA FINAL DE LA CONFERENCIA INTERGUBERNAMENTAL QUE HA ADOPTADO EL TRATADO DE LISBOA firmado el 13 de diciembre de 2007. *Vid*. VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA.

[342] Declaración n. 20 relativa al artículo 16 del TFUE. De hechos, se hace referencia a las excepciones que se contemplaban en la Directiva 95/46/CE (artículo 3, apartado 2 y artículo 13), como también a las excepciones ahora contenidas en el nuevo Reglamento General de Protección de Datos (artículo 2, letra d. y artículo 23). *Vid*. *infra*.

[343] Artículo 39 del TUE: «*De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes*».

[344] *Vid*. Joni HELISKOSKI (2008), «Small arms and light weapons within the Union's pillar structure: An analysis of Article 47 of the EU Treaty», en *European Law Review*, vol. 33, núm. 6, págs. 898-912; Fabio BALDUCCI ROMANO (2015), «La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo», en *Rivista Italiana di Diritto Pubblico Comunitario*, anno XXV, fasc. 6, pág. 1631. Disponible en Internet:

29. El artículo 16 del TFUE establece la base jurídica de un marco jurídico global aplicable a las diferentes actividades de la Unión, ampliando la protección de datos a la PESC. No obstante, la ampliación del campo de aplicación de las normas de protección de datos a la PESC debe tener en cuenta las disposiciones específicas establecidas en el nuevo artículo 39 del TUE[345]. El artículo 39 del Tratado de la Unión deroga al apartado 2 del artículo 16 del TFUE, al establecer que el Consejo establecerá normas específicas sobre la protección de datos personales tratados por los Estados miembros en el ámbito de la PESC y que, en este caso, su aplicación estará sujeta al control de autoridades independientes. El derecho subjetivo a la protección de los datos personales establecido por el artículo 16, apartado 1, seguirá siendo aplicable en este ámbito, pero el procedimiento para la adopción de las normas específicas no implicará al Parlamento Europeo. No obstante, dado que el artículo 39 del TUE establece excepciones únicamente en lo que respecta al tratamiento de datos personales por parte de los Estados miembros, la disposición general del artículo 16 parece seguir siendo plenamente aplicable -incluida la participación del Parlamento Europeo- en el caso del tratamiento de datos personales por las instituciones de la Unión Europea.

30. Sin embargo, en la Declaración n. 21, en el marco de las Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa, se apunta que podrán «*requerirse normas específicas para la protección de datos personales y la libre circulación de dichos datos*» en el área «*de la cooperación judicial en materia penal y de la cooperación policial*» que se basen en el artículo 16 del TFUE, en razón de la naturaleza específica de dichos ámbitos[346]. De hecho, las informaciones en el ELSJ también se intercambian para analizar las amenazas de seguridad, identificar las tendencias de la actividad delictiva o evaluar los riesgos en sectores relacionados.

https://art.torvergata.it/retrieve/handle/2108/184345/367266/Fabio%20Balducci%20Romano.pdf [consulta: 20 de mayo de 2017].

[345] Alfonso SCIROCCO (2008).

[346] Declaración n. 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial: «*La Conferencia reconoce que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos*». *Vid*. VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA. Gloria GONZÁLEZ FUSTER (2014b), «La privacidad en Europa ¿Un debate cada vez más fundamental o cada vez menos?», en *Revista TELOS (Cuadernos de Comunicación e Innovación)*, Madrid, Fundación Telefónica, pág. 4. ISSN: 0213-084X. Disponible en Internet: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2014042309560003&idioma=es [consulta: 06 de marzo de 2016].

31. Combinando al artículo 16 del TFUE y las Declaraciones, siempre en el ámbito de la cooperación policial, el Tratado de Lisboa ha introducido algunas innovaciones, lo que agrava las tensiones con la protección de los derechos y las libertades fundamentales.

32. Según el artículo 87 del TFUE (antiguo artículo 30 del TUE), apartado 1, la Unión «*desarrollará una cooperación policial en la que participen todas las autoridades competentes de los Estados miembros*», con el fin de la «*prevención y en la detección e investigación de infracciones penales*». Se amplió la competencia de la Unión en el ámbito de las técnicas de investigación para la detección de formas graves de delincuencia organizada, estableciendo que el Consejo y el Parlamento, a través del procedimiento legislativo ordinario, pueden adoptar medidas relativas a: «*a) la recogida, almacenamiento, tratamiento, análisis e intercambio de información pertinente; b) el apoyo a la formación de personal, así como la cooperación para el intercambio de personal, los equipos y la investigación científica policial; c) las técnicas comunes de investigación relacionadas con la detección de formas graves de delincuencia organizada*» (apartado 2). En otras palabras, "no se hace ninguna referencia al cumplimiento de las normas sobre protección de datos personales en el caso de tratos efectuados en el ámbito de la cooperación policial", así como la disponibilidad de datos, mediante el intercambio de ellos entre dichas autoridades, lo que «*constituye un retroceso respecto de la normativa anterior a Lisboa*»[347]. También con respecto a la cooperación a nivel operativo, el Tratado establece la posibilidad de adoptar medidas, e incluso en ausencia de unanimidad que se requería normalmente usando el método de la "cooperación reforzada"[348]. En estas áreas, el control realizado por el Parlamento Europeo debería ser capaz de evitar la adopción de actos que ponen en peligro los derechos y libertades de las personas[349].

33. En el marco legal presentado hasta ahora, en referencia al derecho a la protección de datos personales y los riesgos que pueden dar lugar en el ámbito de la cooperación entre las

[347] *Vid*. Alejandro Luis GACITÚA ESPÓSITO (2014: 157). También, *vid*. Stefano CIAMPI (2009), «Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea», en Francesco PERONI, Mitja GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT, págs. 34-100. Disponible en Internet: https://www.openstarts.units.it/dspace/handle/10077/3350 [consulta: 08 de marzo de 2016].

[348] «*El procedimiento específico establecido en los párrafos segundo y tercero no será de aplicación a los actos que constituyan un desarrollo del acervo de Schengen*», artículo 87 del TFUE párrafo final.

[349] *Vid*. en esta misma investigación el apartado sobre Europol, en particular nos referimos a la función de «*apoyar y reforzar la actuación de las autoridades policiales y de los demás servicios con funciones coercitivas de los Estados miembros, así como su colaboración mutua en la prevención de la delincuencia grave que afecte a dos o más Estados miembros, del terrorismo y de las formas de delincuencia que lesionen un interés común que sea objeto de una política de la Unión, así como en la lucha en contra de ellos*» (artículo 88 del TFUE).

fuerzas de seguridad surge la preocupación de que pueda ponerse en discusión el sistema de la plena cooperación de los Estados desarrollada dentro de la UE. En este sentido, la Unión Europea ha ido incrementando gradualmente el número de sistemas de información y bases de datos accesibles para las entidades policiales; en concreto, ha reformado diversos actos legislativos que regulan la recogida de datos personales para usos comerciales y de control transfronterizo, con el fin de permitir a las autoridades policiales acceder a los mismos. Esta preocupación se basa, sobre todo, en lo que respecta a la violación del principio de disponibilidad de los datos y consiguiente violación del principio de finalidad que se vuelven accesibles a todas las autoridades competentes de la UE para los propósitos distintos de aquellos para los que fueron recogidos. Como se desprende del análisis del Derecho de la Unión, esta dificultad se ve agravada por la falta de construcción de un marco coherente y unificado para el derecho a la protección de datos personales dentro de la misma.

34. En conclusión, el artículo 16 del TFUE, además de marcar una consolidación importante y visible en el Derecho primario de la Unión Europea del *acquis* sobre protección de datos desarrollado en Europa durante los últimos años, señala algunos elementos cruciales del derecho fundamental a la protección de los datos personales, en el contexto de una mayor protección de los derechos fundamentales. Por otro lado, encuentra un reconocimiento explícito en el Tratado y desarrolla instrumentos para una mayor y más homogénea protección de datos en las diferentes actividades de la Unión Europea y se prevé, sin embargo, que el cumplimiento sea garantizado y bajo el control de autoridades independientes. Este reconocimiento resulta importante, ya que permite el cambio a un régimen jurídico único, y por lo tanto la superación de la brecha entre los antiguos pilares primero y tercero.

35. En esta perspectiva, los nuevos instrumentos establecidos en el Tratado de Lisboa representan un desafío para la reglamentación europea de protección de datos en el siglo XXI. El primer desafío está relacionado con los esfuerzos necesarios para hacer frente a las nuevas amenazas a la privacidad; a saber, la creciente demanda de seguridad[350] y las inmensas posibilidades que ofrecen las nuevas tecnologías que amenazan la privacidad. Un segundo desafío para la legislación de protección de datos de la UE es seguir siendo una buena práctica global para la protección de datos, lo que significa convertirse en un modelo

[350] En particular, en virtud de la supresión de los pilares, se extiende también la protección de los datos a la cooperación judicial y policial.

de regulación preferido de la privacidad a nivel global, prevaleciendo sobre otros competidores, en particular el modelo de privacidad estadounidense.

36. A través de la asignación de valor jurídico vinculante a la Carta, con particular atención al artículo 8 (*vid*. *infra*), y la introducción del artículo 16 del TFUE, el derecho a la protección de datos personales se ha convertido así, al mismo tiempo, en un derecho fundamental autónomo y un objetivo de la Unión. El artículo 16 sirvió de base jurídica para la adopción de la reforma integral de las normas de protección de datos en 2016, es decir, el Reglamento General de Protección de Datos y la Directiva de protección de datos para las autoridades policiales y de justicia penal (*vid. infra*).

2.2. La realización del ELSJ entre los límites a la protección de los datos personales y la garantía de un elevado nivel de seguridad

37. El espacio común europeo, que nace por la exigencia política para lograr la paz entre los Estados soberanos, después de la Segunda Guerra Mundial, comenzó su cursocon el establecimiento del mercado único. Este mercado único, de hecho, comienza a construir un primer "espacio público común", capaz de superar las rigideces de las fronteras estatales.

38. Desde el Tratado de Maastricht de 1992, en el que se avanza en la consecución del reconocimiento de los derechos fundamentales en la Unión Europea, hemos tenido la superación del originario enfoque meramente mercantil, donde la Unión, por lo tanto, ya no es sólo un espacio económico, sino un espacio en el que la gente realmente tiene la oportunidad de moverse libremente en seguridad a través, de hecho, de un espacio legal armonizado. La Unión Europea no pretende ya solamente una unión monetaria y económica, sino una Unión en Derechos de los ciudadanos comunitarios, donde la libertad, la democracia y los derechos y libertades fundamentales sean la locomotora de su progreso. Este propósito, ha dado como resultado la creación del ELSJ, por el Tratado de Maastricht

y desarrollado antes en los programas de Tampere (1999-2004)[351] y de La Haya (2004-2009)[352].

39. Entre las 10 prioridades del Programa de La Haya, «*se pretende encontrar el equilibrio adecuado entre la protección de la vida privada y la seguridad al compartir información,* (…) *un equilibrio en el respeto de los derechos fundamentales, y particularmente en el respeto a la privacidad y los datos personales*» con la exigencia de la afirmación de que el intercambio de información debería regirse por el "principio de disponibilidad" entre autoridades policiales, judiciales y cuerpos de seguridad guardando un equilibrio adecuado entre derecho a la intimidad y seguridad[353].

[351] Sobre los desarrollos del ELSJ, *vid*. David ORDÓÑEZ SOLÍS (2003), «El espacio judicial de libertad, seguridad y justicia en la Unión Europea», en *Revista de Estudios Políticos*, núm. 119, págs. 447-484. ISSN 0048-7694. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=496725 [consulta: 11 de marzo de 2016]. «*En el Consejo Europeo celebrado en Tampere los días 15 y 16 de octubre de 1999 se acordaron las orientaciones y prioridades políticas que debían guiar la creación de un espacio de libertad, seguridad y justicia. La acción de la Unión Europea se centraba en cuatro áreas: la colaboración con los países de origen de la emigración; la creación de un sistema común de asilo; el desarrollo de una política de integración para los nacionales de terceros Estados* (…)*; finalmente se trataba de combatir la inmigración irregular, gestionando más eficazmente los flujos migratorios*». Un punto de inflexión del desarrollo de las medidas previstas en el Programa de Tampere se produce después los atentados terroristas de Nueva York el 11 de septiembre de 2001, Madrid el 11 de marzo de 2004 y Londres el 7 de julio de 2005. Estos atentados, «*perturban las prioridades normativas de las instituciones comunitarias y las centra en regular aspectos relativos a la seguridad por encima de otras consideraciones dentro del espacio europeo y en mejorar la efectividad del control de las personas que pretenden acceder a dicho espacio*». En Andreu OLESTI RAYO (2008), «Las políticas de la Unión Europea relativas al control en las fronteras, asilo e inmigración», en *Revista de Derecho Constitucional Europeo*, núm. 10, págs. 14-15. ISSN 1697-7890. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3013952 [consulta: 11 de marzo de 2016]; Pedro GARRIDO RODRÍGUEZ (2012), *Inmigración y diversidad cultural en España. Un análisis histórico desde la perspectiva de los derechos humanos*, Salamanca, Ediciones Universidad de Salamanca, págs. 209 y ss.

[352] En noviembre de 2004, el Consejo Europeo adoptó un nuevo programa de acción quinquenal: el Programa de La Haya. EL PROGRAMA DE LA HAYA: CONSOLIDACIÓN DE LA LIBERTAD, LA SEGURIDAD Y LA JUSTICIA EN LA UNIÓN EUROPEA, *Diario Oficial de la Unión Europea*, C 53 de 3.3.2005, págs. 1–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52005XG0303(01) [consulta: 14 de marzo de 2016].

[353] *Vid*. José Francisco ETXEBERRIA GURIDI (2009), «Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo», en *Eguzkilore*, San Sebastián, núm. 23, págs. 351-366. Disponible en Internet http://www.ehu.eus/documents/1736829/2176697/26+Etxeberria.pdf [consulta: 16 de marzo de 2016]; Antonio M. DÍAZ FERNÁNDEZ (2012), «Evolución de la cooperación europea en inteligencia», en *Varia Historia*, Belo Horizonte, vol. 28, núm. 47, págs. 177 y ss. Disponible en Internet: http://www.scielo.br/pdf/vh/v28n47/08.pdf [consulta: 14 de marzo de 2016]; Fernando MARTÍNEZ PÉREZ y María POZA CISNEROS (2013a), *El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm*, 5ª edición, Madrid, Consejo General del Poder Judicial, págs. 98. Disponible en Internet: http://www5.poderjudicial.es/cvcp12-13/CVCP13-09-ES.pdf [consulta: 17 de marzo de 2016]. Para ejecutar el Programa de La Haya la Comisión presentó una Comunicación al Consejo y al Parlamento Europeo detallando las diez prioridades en el plazo de cinco años. El principio de disponibilidad de la información aparece formulado por primera vez en la Comunicación cuando entre las cuestiones relativas a la primera prioridad "Derechos fundamentales y ciudadanía: crear políticas de gran alcance" se afirmaba la necesidad de «*prestar especial atención a la protección de los datos personales, cuyo carácter de derecho fundamental con entidad propia, distinto del derecho a la intimidad, se reconoce en la Carta de derechos fundamentales y en la Constitución*»; y en la segunda prioridad en relación a la lucha al terrorismo, «*exige la atención de la Unión es la cooperación entre las distintas autoridades competentes de los Estados miembros, especialmente a la hora de intercambiar información pertinente para la investigación de actividades terroristas*». En la prioridad

40. Tras los programas de Tampere y La Haya, el Consejo Europeo adoptó en diciembre de 2009 el programa plurianual en el ámbito del ELSJ para el periodo 2010-2014: el Programa de Estocolmo. Uno de los objetivos clave establecidos por el Programa de Estocolmo (artículo 68 del TFUE)[354], que establece un plan de trabajo para la Unión Europea en el ELSJ, es una mejor protección de los datos personales en la Unión. En el Programa «*se pretende que la Unión Europea cuente con un único sistema de protección de datos personales que incluya la certificación europea para las tecnologías, productos y servicios que protejan la privacidad*»[355]. En este marco, sin duda, la seguridad TI se convierte en un tema preeminente del Programa de Estocolmo. El Programa trata de conciliar, «*la necesidad del intercambio de datos personales, dando cumplimiento al principio de disponibilidad*»[356], con el debido respeto de la vida privada de las personas, desarrollando sistemas informáticos de gran envergadura en el ELSJ, garantizando un nivel elevado de protección de datos en materia de registro de nombres de los pasajeros a efectos de prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves. También se «*manifiesta la necesidad de crear un marco legislativo coherente de la Unión en materia de transferencia de datos personales a terceros países con fines policiales*»[357].

41. El objetivo establecido por el Programa de Estocolmo[358] de mejorar la protección de los datos personales en la Unión encuentra correspondencia en la CDFUE, después de la

séptima, "Derecho a la intimidad y seguridad en el intercambio de información: lograr el equilibrio adecuado", se añade, que este intercambio de información no es admisible ilimitadamente, sino en el marco de un equilibrio adecuado entre seguridad y vida privada «*respetando plenamente los derechos fundamentales a la intimidad y a la protección de datos, así como el principio de disponibilidad de la información*». En este ámbito, cuando las autoridades policiales u judiciales intercambien información, «*deberán llegar al equilibrio adecuado entre el derecho a la intimidad y la seguridad*». En este contexto, se concreta lo que ha de entenderse por principio de disponibilidad: «(…) *las autoridades de un Estado miembro pondrán a disposición de las autoridades de otro Estado miembro la información que necesiten a efectos represivos, bajo ciertas condiciones*». *Vid*. COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia, Bruselas, 10.5.2005, COM(2005) 184 final. Disponible en Internet: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2009/7286.pdf?view=1 [consulta: 17 de marzo de 2016].

[354] Con arreglo al artículo 68 del TFUE («*El Consejo Europeo definirá las orientaciones estratégicas de la programación legislativa y operativa en el espacio de libertad, seguridad y justicia*»), en sus conclusiones de junio de 2014, el Consejo Europeo definió las orientaciones estratégicas de la programación legislativa y operativa en el ELSJ para los próximos años, que están en consonancia con las prioridades establecidas en la Agenda Estratégica para la UE, que también se aprobó en junio. Las orientaciones estratégicas se basan en los logros alcanzados por el Programa de Estocolmo.

[355] Alejandro Luis GACITÚA ESPÓSITO (2014: 154).

[356] Alejandro Luis GACITÚA ESPÓSITO (2014: 154).

[357] Alejandro Luis GACITÚA ESPÓSITO (2014: 154).

[358] En efecto, el Programa de Estocolmo ha recibido importantes críticas provenientes de las ONG por el profundo impacto que tendrá en el derecho a la privacidad de los ciudadanos europeos los procesos paralelos de un aumento del intercambio de información y la falta de unos estándares más efectivos de protección de datos personales. EUROPEAN CIVIL LIBERTIES NETWORK (2009), *Declaración del ECLN sobre el Programa de Estocolmo de la UE: Oponerse a las prácticas estatales autoritarias y crear una Europa*

entrada en vigor del Tratado de Lisboa[359], en particular en los artículos 7 y 8, donde se encuentran la protección explícita, respectivamente, del derecho al respeto de la vida privada y familiar (así como el hogar y comunicaciones) y el derecho a la protección de los datos personales; ambos derechos que, sobre la base de la disposición en el artículo 6 del TUE, ahora tienen el mismo valor jurídico que los Tratados, y por lo tanto conllevan la obligación jurídica no sólo de la Unión, sino también con respecto a los Estados miembros en la aplicación del derecho de la UE (*vid*. *infra*, artículo 51, apartado 1, de la CDFUE)[360].

42. Con motivo de la adopción del Tratado de Maastricht en el conocido como "tercer pilar" (Título VI) −que se ocupaba del ámbito de justicia y asuntos de interior como parte de la cooperación gubernamental−, la UE sólo irrumpió abiertamente en la problemática conciliación entre la libertad y la seguridad en el Derecho primario u originario, en conexión con el cual la protección de la privacidad adquiría una nueva dimensión a través de la creación de la *ex* Oficina Europea de Policía (Europol).

43. La entrada en vigor del Tratado de Lisboa, elimina la estructura de pilares, tal como se había establecido a partir del Tratado de Ámsterdam[361], firmado en el 1997. Con el

democrática, 15 de abril de 2009. Disponible en Internet: https://stockholm.noblogs.org/post/2009/04/15/declaraci-n-del-ecln-acerca-del-programa-de-estocolmo-de-la-ue/ [consulta: 20 de marzo de 2016].

[359] El Programa de Estocolmo fue la primera iniciativa *post*-Lisboa que determinó la nueva legislación en el ámbito del ELSJ, incluyendo el tratamiento de la información con finalidades de seguridad. Más tarde, el Consejo Europeo y la Comisión concretaron lo previsto en el programa a partir de una Comunicación y una estrategia Europa 2020, con el fin de establecer entre ellas normas de protección de datos dentro del ELSJ. En dicha Comunicación se expone que el impulso principal a la acción de la Unión en este ámbito en los próximos años consistirá en «*progresar en la Europa de los ciudadanos*», con la garantía de que éstos puedan ejercer sus derechos y disfrutar plenamente de las ventajas de la integración europea. En esta línea, la protección de los derechos consagrados en la Carta de los Derechos Fundamentales debería convertirse en el eje de todas las normativas y políticas de la UE. La Comisión aplicará una «*política de tolerancia cero*» frente a las violaciones de la Carta. La Comisión reconoce que «*La Unión debe garantizar la aplicación coherente del derecho fundamental a la protección de datos. Debemos reforzar la posición de la UE en cuanto a la protección de los datos personales en el contexto de todas las políticas de la UE, incluida la represión policial y la prevención de la delincuencia, así como en nuestras relaciones internacionales*». De acuerdo con el Programa de Estocolmo y siguiente Plan de Acción, *vid*. *amplius* COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo, Bruselas, 20.4.2010, COM(2010) 171 final. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0171 [consulta: 06 de marzo de 2015].

[360] Por otra parte, un reconocimiento adicional de tales derechos en el ámbito europeo se encuentra en el artículo 16 del TFUE, que representa, como ya mencionado, la nueva base jurídica para la adopción de toda la legislación de la Unión que tiene como objetivo la protección de datos personales. *Vid*. PROGRAMA DE ESTOCOLMO - UNA EUROPA ABIERTA Y SEGURA QUE SIRVA Y PROTEJA AL CIUDADANO, *Diario Oficial de la Unión Europea*, C 115 de 4.5.2010, págs. 1–38. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010XG0504%2801%29 [consulta: 13 de junio de 2015].

[361] El Tratado de Ámsterdam fue un acuerdo firmado el 2 de octubre de 1997 en la ciudad de Ámsterdam. Entró en vigor el 1 de mayo de 1999. Tras haber sido ratificado por todos los Estados miembros de la Unión Europea, pasando a convertirse en la nueva normativa legal de la Unión Europea, tras revisar el Tratado de Maastricht.

Tratado de Ámsterdam, el llamado "acervo de Schengen" se comunitarizó[362]. En efecto, el Tratado indica en el artículo 1, núm. 8, que: «*la Unión se basa en los principios de libertad, democracia, respeto de los derechos humanos y de las libertades fundamentales y el Estado de Derecho, principios que son comunes a los Estados miembros*»[363]. También, el citado Tratado reconoce competencia al Tribunal de Justicia de la UE para defender los derechos fundamentales, y a partir de allí, el respeto a la vida privada, reconocido en el artículo 8 del CEDH, que adquiere toda su importancia en el ámbito europeo[364].

44. A pesar de este marco legislativo, el régimen de protección de datos de la UE contiene una serie de debilidades y derogaciones que diluyen la capacidad de proteger los derechos de privacidad. El principal inconveniente es que los Estados miembros son obviamente competentes para adoptar decisiones en materia de seguridad nacional, "lo que puede entrar en conflicto con el derecho a la privacidad" cuando se utilicen sofisticados programas de obtención y almacenamiento de datos.

45. Con relación al control jurisdiccional, en el artículo 2, apartado 1, del "Protocolo por el que se integra el acervo de Schengen en el marco de la Unión Europea" del Tratado de Ámsterdam, se establece que «*el Tribunal de Justicia de las Comunidades Europeas ejercerá las competencias que le otorgan las disposiciones aplicables pertinentes de los Tratados. En todo caso, el Tribunal de Justicia no tendrá competencia alguna sobre las medidas o decisiones relativas al mantenimiento de la ley y el orden público así como a la salvaguarda de la seguridad interior*»[365]. En esta línea, dicho Protocolo establece que las Partes Contratantes «*tomando nota de que los acuerdos relativos a la supresión gradual de los controles en las fronteras comunes, firmados en Schengen por determinados Estados miembros de la Unión Europea el 14 de junio de 1985 y el 19 de junio de 1990, así como*

Este último Tratado había previamente establecido de suprimir la estructura de «pilares». *Vid*. Antonio CALONGE VELÁZQUEZ (dir.) (2017), *Derecho Básico de la Unión Europea*, 2ª edición, Granada, Editorial Comares, págs. 41 y ss.

[362] David ORDÓÑEZ SOLÍS (2003: 457 y ss.); Beatriz S. TOMÁS MALLÉN (2014: 219).

[363] TRATADO DE ÁMSTERDAM POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA, LOS TRATADOS CONSTITUTIVOS DE LAS COMUNIDADES EUROPEAS Y DETERMINADOS ACTOS CONEXOS, tal como ha sido firmado el 2 de octubre de 1997 en Ámsterdam. Disponible en Internet: http://www.europarl.europa.eu/topics/treaty/pdf/amst-es.pdf [consulta: 08 de febrero de 2016].

[364] Teresa FREIXES SANJUÁN (2005), «Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales», en *Revista de Derecho Constitucional Europeo*, año 2, núm. 4. Disponible en Internet: http://www.ugr.es/~redce/REDCE4/articulos/02freixes.htm [consulta: 06 de enero de 2016].

[365] TRATADO DE ÁMSTERDAM POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA, LOS TRATADOS CONSTITUTIVOS DE LAS COMUNIDADES EUROPEAS Y DETERMINADOS ACTOS CONEXOS, pág. 94.

los acuerdos relacionados y las normas adoptadas en virtud de los mismos, tienen como finalidad potenciar la integración europea y hacer posible, en particular, que la Unión Europea se convierta con más rapidez en un espacio de libertad, seguridad y justicia»[366]. Podemos decir que, a partir de ahí, el derecho a la protección de datos adquiere una especial relevancia en el ámbito jurídico.

46. No obstante, en el TFUE se establece una importante restricción, ya que el TJUE «*no será competente para comprobar la validez o proporcionalidad de las operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni para pronunciarse sobre el ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior*» (artículo 276). Sin embargo, esta restricción no influye con los controles internos de cada Estado. Por lo tanto, los tribunales de cada Estado miembro pueden decidir en definitiva sobre la proporcionalidad de actividades efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro que tengan como finalidad el mantenimiento del orden público y de la salvaguardia de la seguridad interior[367].

47. Nos interesa remarcar, que la Unión y los Estados miembros disponen formalmente de "competencia compartida" en la construcción del denominado ELSJ[368], «*dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicos de los Estados miembros*»[369], que tiene, entre sus objetivos reconocidos por el artículo 67 (antiguo artículo 61 TCE y antiguo artículo 29 TUE), Título V del TFUE, que la Unión constituye «*un espacio de libertad, seguridad y justicia dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicos de los Estados miembros*» (apartado 1).

48. Quedando dentro los objetivos asignados al ELSJ que se detallan en el artículo 67 del TFUE, la Unión se esforzará por garantizar: «*un nivel elevado de seguridad mediante*

[366] TRATADO DE ÁMSTERDAM POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA, LOS TRATADOS CONSTITUTIVOS DE LAS COMUNIDADES EUROPEAS Y DETERMINADOS ACTOS CONEXOS, pág. 93.
[367] Artículo 276 del TFUE. *Vid*. Ricardo ALONSO GARCÍA (2010), «Lisboa y el Tribunal de Justicia de la Unión Europea», en *Papeles de Derecho Europeo e Integración Regional*, Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense, núm. 1, pág. 8-9. Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2013-11-07-lisboa%20y%20el%20derecho.pdf [consulta: 07 de enero de 2016].
[368] *Vid*. artículo 4, apartado j), del TFUE.
[369] Kristiina MILT (2019).

medidas de prevención de la delincuencia (…)*, medidas de coordinación y cooperación entre autoridades policiales y judiciales y otras autoridades competentes, así como mediante el reconocimiento mutuo de las resoluciones judiciales en materia penal y, si es necesario, mediante la aproximación de las legislaciones penales*»[370] (apartado 3). Por tanto, con respecto al ELSJ, la Unión Europea está comprometida que se adopten medidas legislativas que deben respetar «*la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos*» de las personas que se encuentran dentro de la Unión[371]. Además, dentro de las políticas de contraste al terrorismo, la policía y las fuerzas de seguridad deben respetar "la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos de las personas" y, en particular, su privacidad y datos personales.

49. La importancia de los derechos y de las libertades fundamentales de las personas es, claramente, parte integral de la concepción del espacio común europeo, en línea con la idea de construir una verdadera comunidad de derecho[372]. En este sentido, el respeto de los derechos y la legalidad en el ejercicio del poder son un marco legal de protección, confirmado por la adopción de la CDFUE, legalmente vinculante, así como en la prevista adhesión del UE al CEDH[373]. Además, los Estados miembros tendrán que crear un comité permanente en el Consejo con objeto de garantizar dentro de la Unión «*el fomento y la intensificación de la cooperación operativa en materia de seguridad interior*»[374], y la posibilidad de organizar entre ellos y bajo su responsabilidad «*formas de cooperación y coordinación en la medida en que lo estimen apropiado, entre los servicios competentes de sus administraciones responsables de velar por la seguridad nacional*» (artículo 73 del TFUE). El texto del Tratado, sin embargo, señala que esas formas aún serían bajo la plena responsabilidad de los Estados, reiterando la exclusión de una acción autónoma de la UE.

[370] Beatriz TOMÁS MALLÉN (2014: 220).
[371] Artículo 2 del TUE: «*La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías. Estos valores son comunes a los Estados miembros en una sociedad caracterizada por el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres*».
[372] El artículo 75 del TFUE establece también que, si es necesario para lograr los objetivos establecidos en el artículo 67, en relación con la prevención y la lucha contra el terrorismo y las actividades relacionadas, «*el Parlamento Europeo y el Consejo definirán mediante reglamentos, con arreglo al procedimiento legislativo ordinario, un marco de medidas administrativas sobre movimiento de capitales y pagos, tales como la inmovilización de fondos, activos financieros o beneficios económicos cuya propiedad, posesión o tenencia ostenten personas físicas o jurídicas, grupos o entidades no estatales*».
[373] Puede citarse en este sentido la ASOCIACIÓN PRO DERECHOS HUMANOS DE ESPAÑA (2011), *La adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos: su impacto institucional sobre la política y la ciudadanía europea. Jornada de expertos*, Madrid, 21 de octubre de 2011, págs. 67.
[374] Artículo 71 del TFUE (antiguo artículo 36 del TUE).

50. Por último, el Tratado de Lisboa establece que el Parlamento Europeo y el Consejo[375], de conformidad con el procedimiento legislativo ordinario, podrán establecer "normas mínimas" relativas a la definición de los delitos y las sanciones en cuanto a la dimensión transnacional de los delitos, en primer lugar, el terrorismo, la delincuencia informática y la delincuencia organizada[376]. La razón subyacente de este enfoque es que los Estados miembros no pueden abordar eficazmente solos las amenazas transnacionalesy que, por lo tanto, hace falta proporcionar herramientas necesarias a nivel europeo, e infraestructuras y entornos de coordinación en ~~el~~ que las autoridades nacionales colaboren para hacer frente a los retos comunes de manera efectiva. Sin embargo, de acuerdo con el TFUE, el Título V sobre el ELSJ «*se entenderá sin perjuicio del ejercicio de las responsabilidades que incumben a los Estados miembros en cuanto al mantenimiento del orden público y la salvaguardia de la seguridad interior*»[377].

51. Esta última línea, de hecho, se destaca además en relación con el TUE que excluye al artículo 4, apartado 2, de manera clara y explícita la competencia de la Unión en materia de orden público y seguridad nacional y se especifica, aún más, a continuación, el carácter absoluto de esta disposición, indicando que la seguridad nacional sigue siendo prerrogativa de cada Estado miembro: «*La Unión respetará la igualdad de los Estados miembros ante los Tratados, así como su identidad nacional, inherente a las estructuras fundamentales políticas y constitucionales de éstos, también en lo referente a la autonomía local y regional. Respetará las funciones esenciales del Estado, especialmente las que tienen por objeto garantizar su integridad territorial, mantener el orden público y salvaguardar la seguridad nacional. En particular, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro*». Este reconocimiento de la competencia exclusiva del Estado tiene consecuencias prácticas hasta el nivel de la legislación secundaria. Por ejemplo, la Directiva UE sobre protección de datos (95/46/CE), artículo 13, apartado 1, permitía a los Estados miembros «*adoptar medidas legales para limitar el alcance de las obligaciones y los derechos* (…) *cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública;* (…)». Estas excepciones también fueron recordadas por el reciente RGPD (UE) 2016/679 en su

[375] La estrategia securitaria de la UE se ha sustanciado principalmente a través de la PESC, el antiguo segundo pilar que sigue rigiéndose por las reglas de cooperación intergubernamental, aunque también se ha apoyado en la política comunitaria de interior y en el ESLJ, donde el papel del Parlamento y de la Comisión son más notorios.
[376] Artículo 83 del TFUE (antiguo artículo 31 del TUE).
[377] Artículo 72 del TFUE (antiguo artículo 64, apartado 1, del TCE y antiguo artículo 33 del TUE).

considerando 16: «*El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión*». Siguiendo en la misma línea de limitaciones, el mismo Reglamento contempla limitaciones también en el artículo 23, apartado 1: «*El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos* (…)*, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro* (…)» (*amplius*, *vid.* Capítulo V).

52. Es evidente que la elección de la introducción del artículo 4 del TUE pretende ir más allá y eliminar cualquier duda sobre la posibilidad de cualquier acción de la UE en la materia[378]. Los Estados miembros han intentado remachar su absoluta prerrogativa a actuar en materia de seguridad nacional, poniendo el artículo 4 en una posición privilegiada, encontrando origen común en la relación de delimitar de la manera más clara y nítida la demarcación de competencias entre la Unión y los Estados en el campo de la seguridad

[378] Clemens LADENBURGER (2008), «The Resources of European Security-Developing the EU Treaty Bases for Police Cooperation and Judicial Cooperation in Criminal Matters», en *European Review of Public Law*, Esperia Publications Ltd, vol. 20, núm. 1, pág. 143.

nacional[379], haciendo de éste un área de ejercicio reservado exclusivamente a ellos[380], no sólo para el ELSJ, sino en referencia a todo el Tratado.

53. El Tratado representa en muchos aspectos un progreso en el proceso de integración europea. Sin embargo, no ha marcado una discontinuidad con respecto a la reserva de la soberanía nacional para los asuntos relacionados con las políticas de seguridad. Se puede decir que las prerrogativas de los Estados como parte de su protección de seguridad es incluso reforzada por el nuevo Tratado, que sigue siendo en último extremo una cuestión fundamentalmente estatal donde escasean los controles comunitarios[381]. Así, por poner un ejemplo, incluso el intercambio de información que a veces se ha acordado en esa lucha antiterrorista no es una obligación cuando un Estado considere que su divulgación puede ser contraria a los intereses esenciales de su propia seguridad[382].

[379] Debe tenerse presente que el artículo 222 del TFUE establece, entre otras cosas, una "cláusula de solidaridad" que permita a la Unión y a los Estados miembros a tomar medidas conjuntas si uno de ellos se convierte en objeto de un ataque terrorista. También pueden actuar conjuntamente si un Estado miembro es «*víctima de una catástrofe natural o de origen humano*». En este ámbito se adoptó la DECISIÓN DEL CONSEJO de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (2014/415/UE), *Diario Oficial de la Unión Europea*, L 192 de 1.7.2014, págs. 53–58. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32014D0415 [consulta: 09 de enero de 2016]. La Unión movilizará «*todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros, para: a) prevenir la amenaza terrorista en el territorio de los Estados miembros; proteger a las instituciones democráticas y a la población civil de posibles ataques terroristas; prestar asistencia a un Estado miembro en el territorio de éste, a petición de sus autoridades políticas, en caso de ataque terrorista*». Parece oportuno señalar que, a raíz de los ataques terroristas en París el 13 de noviembre de 2015, el presidente francés Hollande, considerando los ataques terroristas reales actos de agresión armada, ha pedido la activación de la cláusula de solidaridad prevista en el artículo 42 del TUE, según el cual, «*si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las Naciones Unidas*». «*Las modalidades de aplicación por la Unión de la presente cláusula de solidaridad serán definidas mediante decisión adoptada por el Consejo, a propuesta conjunta de la Comisión y del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad*», previa información al Parlamento Europeo. Cuando dicha decisión tenga repercusiones en el ámbito de la defensa, el Consejo Europeo y el Consejo adoptarán por unanimidad las decisiones (artículo 222, apartado 3, del TFUE y artículo 31, apartado 1, del TUE). El Tratado permite a la Unión usos de medios civiles y militares «*en misiones fuera de la Unión que tengan por objetivo garantizar el mantenimiento de la paz, la prevención de conflictos y el fortalecimiento de la seguridad internacional, conforme a los principios de la Carta de las Naciones Unidas*» (artículo 42, apartado 1, del TUE). El artículo 43 del TUE especifica que estas misiones podrán contribuir a la lucha contra el terrorismo, incluido el apoyo a terceros países en la lucha contra el terrorismo en sus territorios.

[380] A pesar de que el Tratado de Lisboa consigue la supresión de los regímenes diferenciados de decisión, los llamados pilares, y, por lo tanto, la generalización del método comunitario genera fuerte criticidad en la gestión de estas políticas a causa de las resistencias de los Estados a ceder ámbitos de soberanía en las áreas donde los intereses nacionales no siempre coinciden con la de los otros Estados europeos. De hecho, el poder constituye una gran parte del núcleo duro de la soberanía y un punto de referencia para su supervivencia de los Estados.

[381] Rosario SERRA CRISTÓBAL (2016: 490).

[382] Artículo 8 de la DECISIÓN DEL CONSEJO de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (2014/415/UE). De hecho, las respuestas a los ataques yihadistas perpetrados en Europa en los últimos años han dado lugar a una respuesta decidida y protagonizada de forma principal por los Estados que han visto en riesgo su propia seguridad.

54. El peligro de esta elección es claro si se considera que, como se mencionó anteriormente, no existe una definición positiva universalmente acordada sobre lo que constituye seguridad nacional o términos estrechamente relacionados como "seguridad interna" o "seguridad del Estado." El concepto de seguridad nacional varía de Estado a Estado. Por lo tanto, dado que no existe una definición uniforme de seguridad nacional[383], con límites legales estables y definidos, existe el riesgo de que, en ausencia de criterios fijos y verificables, las disposiciones en cuestión sean utilizadas por los Estados de manera arbitraria para recuperar parte de sus soberanías, poniendo en peligro los derechos y las libertades individuales.

55. En el ámbito de la UE, la responsabilidad principal de diseñar el sistema legal en materia de seguridad nacional y de su aplicación a nivel nacional recae en cada Estado miembro. La Unión se ha embarcado en la armonización de los sistemas jurídicos con el fin de lograr una mayor eficacia en la lucha contra el terrorismo[384], al igual que en una cooperación policial y judicial en materia penal, por la aplicación de las normas recaída en el Título V sobre el ELSJ[385]. Los evocados artículos del Tratado parecen tener sus raíces en la razón común de la "delimitación de las competencias entre la Unión y los Estados en el campo de la seguridad nacional", haciendo de éste un área de ejercicio reservado exclusivamente a ellos. De hecho, tal poder constituye parte relevante de la soberanía, y los Estados, a continuación, la perciben como un punto de referencia para su supervivencia[386].

[383] Hay algunos Estados que han definido la seguridad nacional a nivel regional, entre ellos Suecia en su Código Penal, Hungría en la Ley CXXV de 1995 sobre los Servicios de Seguridad Nacional, España en la Ley de Defensa Nacional de 2005, el Reino Unido en la *Security Service Act 1989*. Italia, no prevé una definición explícita de "seguridad nacional", sin embargo, esta definición puede deducirse sobre la de secreto de Estado en el artículo 39, apartado 1, de la Ley 124/2007. *Vid*. Sandra COLIVER (2012), «National Security and the Right to Information», en *Right2INFO.org*, pág. 6, nota 11. Disponible en Internet: https://www.opensocietyfoundations.org/sites/default/files/coliver-nsp-pace-20121220.pdf [consulta: 11 de enero de 2016].

[384] Rosario SERRA CRISTÓBAL (2016: 489, nota 6).

[385] El artículo 83 del TFUE (antiguo artículo 31 TUE) se refiere explícitamente al terrorismo como forma grave de delincuencia: «*El Parlamento Europeo y el Consejo podrán establecer, mediante directivas adoptadas con arreglo al procedimiento legislativo ordinario, normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes. Estos ámbitos delictivos son los siguientes: el terrorismo, la trata de seres humanos y la explotación sexual de mujeres y niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada*».

[386] El Tratado también contiene disposiciones de derogación general para asegurar el estricto sentido a los Estados el control sobre su propia seguridad y el orden público. Se trata de los artículos 346 y 347 del TFUE. El primero de ellos presenta dos tipos de excepciones basadas en la seguridad nacional: «*a) ningún Estado miembro estará obligado a facilitar información cuya divulgación considere contraria a los intereses esenciales de su seguridad; b) todo Estado miembro podrá adoptar las medidas que estime necesarias para la protección de los intereses esenciales de su seguridad y que se refieran a la producción o al comercio de armas, municiones y material de guerra; estas medidas no deberán alterar las condiciones de competencia en*

En efecto, existe el riesgo de que, en nombre de la seguridad nacional y el orden público, "los Estados miembros puedan poner en peligro los derechos y las libertades de sus ciudadanos", como el derecho a la protección de privacidad[387].

3. La protección de datos como derecho fundamental autónomo: la Carta de los Derechos Fundamentales de la Unión Europea

56. La Unión Europea ha sido fundada con el fin de crear un mercado común basado en la libre circulación de personas, mercancías, servicios y capitales. El sistema jurídico comunitario pensado inicialmente en la integración económica no establecía, por tanto, disposiciones específicas en relación con los derechos fundamentales, y tampoco la privacidad. A este vacío legal, desde principios de los años setenta, pone remedio la jurisprudencia del TJUE, que, apoyándose en las tradiciones constitucionales de los Estados miembros y los principios establecidos en el CEDH, ha reconocido la protección de los derechos humanos como parte integrante del Derecho comunitario[388]. Por tanto, mucho antes de la adopción de una legislación que proporcionaría el reconocimiento adecuado de los derechos humanos y la regulación específica de la privacidad, Europa ha tomado medidas para proteger de manera efectiva los principios fundamentales de la persona, principalmente

el mercado interior respecto de los productos que no estén destinados a fines específicamente militares». El artículo 347, sin embargo, se refiere a la posibilidad de que los Estados adopten «*disposiciones necesarias para evitar que el funcionamiento del mercado interior resulte afectado por las medidas que un Estado miembro pueda verse obligado a adoptar en caso de graves disturbios internos que alteren el orden público, en caso de guerra o de grave tensión internacional que constituya una amenaza de guerra, o para hacer frente a las obligaciones contraídas por el mismo para el mantenimiento de la paz y la seguridad internacional*». En este sentido, José Manuel CORTÉS MARTÍN (2010), «Jurisprudencia del Tribunal de Justicia de la Unión Europea. Septiembre–Diciembre 2009», en *Revista de Derecho Comunitario Europeo*, año 14, núm. 35, págs. 274-275. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3233868 [consulta: 25 de mayo de 2015].

[387] Esta situación presenta un límite adicional dada la ausencia de un mecanismo eficaz para sancionar a los Estados culpables de tales violaciones, ya que, el procedimiento del artículo 7 del Tratado UE constituye una posibilidad floja, que responde a la lógica de oportunidad política, en lugar de jurídica.

[388] En las sentencias de 12 de noviembre de 1969, asunto 29/69, *Erich Stauder contra City of Ulm-Sozialamt* y de 14 de mayo de 1974, asunto 4/73, *J. Nold, Kohlen-und Baustoffgrosshandlung contra Comisión Europea*, cuando el TJCE afirma claramente que la protección de los derechos fundamentales forma parte integral del Derecho comunitario, garantizando su eficacia mediante su inviabilidad directa y el reenvío prejudicial. Esta técnica, por su flexibilidad, permitió incorporar derechos fundamentales de diverso origen (de las Constituciones de los Estados miembros, de Tratados internacionales o del propio Derecho comunitario) al ordenamiento jurídico comunitario, adecuándolos a las características de éste. *Vid*. Teresa PAREJO NAVAJAS (2010), «La Carta de los derechos fundamentales de la Unión Europea», en *Derechos y Libertades: revista de filosofía del derecho y derechos humanos*, núm. 22, época II, págs. 211-212. ISSN: 1133-0937. Disponible en Internet: https://e-archivo.uc3m.es/handle/10016/14569 [consulta: 29 de mayo de 2015]. También *vid*. Roberto MASTROIANNI (2009), «La tutela dei diritti fondamentali tra diritto comunitario e Costituzioni nazionali», en *Convegno Corte di Cassazione "La tutela dei diritti fondamentali tra Corte costituzionale, Corti europee e giudice nazionale"*, Roma, 21 gennaio 2009, pág. 6. Disponible en Internet: www.europeanrights.eu/public/commenti/relazione_Prof1._Mastroianni.doc [consulta: 01 de junio de 2015].

a través de la jurisprudencia de su Tribunal. Pero el mérito de la consagración formal de los derechos humanos dentro de la legislación comunitaria no es sólo de la jurisprudencia del TJUE. Esta consagración, de hecho, fue posible con el nacimiento de la Unión Europea en 1993 por el TUE (conocido también como Tratado de Maastricht)[389].

57. Este último, después de desarrollar el principio de respeto de los derechos fundamentales por parte del TJUE y haber consagrado el mismo artículo 6 del TUE (*cfr. supra*), finalmente se ha provisto de un instrumento autónomo de afirmación de esos derechos. El reconocimiento definitivo de la protección de los datos como derecho fundamental se tiene el 7 de diciembre 2000, cuando Parlamento Europeo, Consejo y Comisión proclamaron solemnemente en Niza la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE, Carta de Niza o Carta)[390].

58. Tras ser revisada, fue proclamada de nuevo en 2007[391] y contemplada como el embrión de una futura Constitución de la Unión Europea. Además de reconocer el derecho más general a la privacidad, tutela de modo específico y expreso el derecho a la protección de los datos personales, dándole así la autonomía jurídica plena[392]. Por lo tanto, se puede decir que el derecho a la protección de los datos de carácter personal, en sus múltiples

[389] TRATADO DE LA UNIÓN EUROPEA, *Diario Oficial*, n. C 191 de 29/07/1992, págs. 0001 - 0110. Disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:11992M/TXT [consulta: 02 de junio de 2015].

[390] En el Consejo Europeo de Colonia de 1999 se otorgó a un órgano *ad hoc* llamado Convención "*Convention*" (presidido por Alemania) el mandato de redactar el proyecto de la Carta. Éste se constituyó en diciembre de 1999 y aprobó el proyecto el 2 de octubre del 2000, el mismo que días después, habría de ser aprobado por el Consejo de Europa de Biarritz el 13 y 14 de octubre, mediante acuerdo unánime, transmitiéndolo al Parlamento Europeo y a la Comisión. El Parlamento Europeo dio su acuerdo el 14 de noviembre de 2000 y la Comisión, el 6 de diciembre de 2000. Finalmente, los Presidentes del Parlamento Europeo, del Consejo y de la Comisión, en nombre de sus instituciones, firmaron y proclamaron la Carta el 7 de diciembre de 2000 en Niza. *Vid*. Montserrat PI LLORENS (2001), *La Carta de los derechos fundamentales de la Unión Europea*, Edicions Universitat Barcelona, págs. 79 y ss.; Cristina HERMIDA DEL LLANO (2005: 227 y ss.); Teresa PAREJO NAVAJAS (2010: 215 y ss.); Ana GARRIGA DOMÍNGUEZ (2016), *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, págs. 158 y ss.

[391] Después de un proceso complejo, la Carta fue proclamada en Estrasburgo, el 12 de diciembre de 2007. Una vez ratificado el Tratado de Lisboa, la Carta es legalmente vinculante para todos los países excepto para Polonia y el Reino Unido. *Vid*. COMISIÓN EUROPEA - Comunicado de prensa (2007), Carta de los Derechos Fundamentales: los Presidentes de la Comisión Europea, del Parlamento y del Consejo firman y proclaman solemnemente la Carta en Estrasburgo, IP/07/1916, Bruselas, 12 de diciembre de 2007. Disponible en Internet: http://europa.eu/rapid/press-release_IP-07-1916_es.htm [consulta: 02 de junio de 2015].

[392] Varios han sido los intentos por los estudiosos para justificar la inclusión de un derecho autónomo a la protección de datos personales en la Carta de Niza. Según algunos, la decisión de dedicar específicamente este derecho es funcional para llevar a la Directiva de 1995 a una perspectiva de la protección de los derechos humanos. La principal objeción contra esta reconstrucción es que sería inaceptable que un nuevo derecho haya sido reconocido en el derecho de la UE sólo con el fin de justificar a posteriori la legislación ya existente. Paul DE HERT, Serge GUTWIRTH (2009), «Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action», in Serge GUTWIRTH and others (eds.), *Reinventing Data Protection?*, Springer Netherlands, pág. 9. En contra Orla LYNSKEY (2014: 3).

facetas, es totalmente protegido a nivel supranacional como un derecho fundamental de la persona[393].

59. La CDFUE resultó innovadora porque "reconoce por primera vez" como derechos fundamentales el derecho a la protección de datos. Sin embargo, tenemos que aclarar que la Carta no introduce *ex novo* una tutela europea o comunitaria de los derechos fundamentales, de una manera más limitada, lleva una contribución a una ya arraigada y consolidada realidad en la Unión Europea. No obstante, a pesar del carácter declarativo de las normas que la componen, la Carta, en su conjunto, parece una obra original por la elección de las normas que ha incluido, excluyendo otras. En este sentido, la Carta ha solucionado el problema de la identificación de un catálogo escrito de los derechos fundamentales protegidos por la Unión Europea, proporcionando, por lo tanto, cierta relevancia normativa ante el Tribunal de Justicia[394].

60. Con la proclamación de la Carta tenemos un cambio de perspectiva en el proceso de integración europea: de la lógica de mercado a la lógica de los derechos[395]. Incorpora "toda la gama de derechos civiles, políticos, económicos y sociales de los ciudadanos europeos", al sintetizar las «*tradiciones constitucionales y las obligaciones internacionales comunes a*

[393] Sobre la CDFUE existe una copiosa bibliografía, entre otros véase Juan Antonio CARRILLO SALCEDO (2001), «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», en *Revista de Derecho Comunitario Europeo*, núm. 9, págs. 7-26; Alberto A. HERRERO DE LA FUENTE (coord.) (2003), *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*, Fundación Rei Afonso Henriques, págs. 267; Carlos RUÍZ MIGUEL (2004), *Estudios sobre la Carta de los Derechos Fundamentales de la Unión Europea*, Universidad de Santiago de Compostela, págs. 246; Ricardo ALONSO GARCÍA, Daniel SARMIENTO (2006), *La Carta de los Derechos Fundamentales de la Unión Europea: explicaciones, concordancias, jurisprudencia*, Madrid, Editorial Civitas, págs. 472; Martin ARACELI MANGAS (dir.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA, págs. 934. Disponible en Internet: http://www.fbbva.es/TLFU/dat/DE_2008_carta_drechos_fundamentales.pdf [consulta: 06 de diciembre de 2015]; Teresa PAREJO NAVAJAS (2010); Silvio GAMBINO (2010), «Jurisdicción y justicia entre Tratado de Lisboa, Convenio Europeo de Derechos Humanos y ordenamientos nacionales», en *Revista de Derecho Constitucional Europeo*, año 7, núm. 13. Disponible en Internet: http://www.ugr.es/~redce/REDCE13/articulos/04Gambino.htm [consulta: 15 de diciembre de 2015]; Cristina BLASI CASAGRAN (2010), «La protección de los Derechos Fundamentales en el Tratado de Lisboa», en *Quaderns de treball*, Institut Universitari d'Estudis Europeus, núm. 51. Disponible en Internet: http://ddd.uab.cat/record/77369/ [consulta: 18 de diciembre de 2015].

[394] Raffaele BIFULCO, Marta CARTABIA, Alfonso CELOTTO (a cura di) (2001), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, Il Mulino, págs. 12-15.

[395] Los principios contenidos en la Carta marcan un importante cambio de perspectiva en la política de la UE sobre los derechos fundamentales. En la Directiva 95/46/CE, la protección de los derechos fundamentales es funcional a la búsqueda de objetivos económicos, en la Carta de Niza son protegidos en sí mismos. Por lo tanto, se pasa de desarrollo de la comunidad europea como "unión económica y monetaria", que se centra en la libertad de circulación de personas, capitales, bienes y servicios, a una "Europa de los derechos de los ciudadanos". Gianpiero Paolo CIRILLO (2004), *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, Cedam, 2004, pág. 5; Silvia MELCHIONNA (2004), «I principi generali», en Riccardo ACCIAI (a cura di), *Il diritto alla protezione dei dati personali*, Rimini, Maggioli Editore, 2004, pág. 32.

los Estados miembros»[396]. Los derechos descritos en la Carta se dividen en seis títulos: Dignidad, Libertades, Igualdad, Solidaridad, Ciudadanía y Justicia[397].

3.1. Problema de definir un "equilibrio europeo" entre los derechos individuales a la protección de datos y las necesidades de seguridad de los Estados

61. El Preámbulo de la CDFUE[398] afirma lo siguiente: «*Consciente de su patrimonio espiritual y moral, la Unión está fundada sobre los valores indivisibles y universales de la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y el Estado de Derecho. Al instituir la ciudadanía de la Unión y crear un espacio de libertad, seguridad y justicia, sitúa a la persona en el centro de su actuación.* (…) *La presente Carta reafirma, dentro del respeto de las competencias y misiones de la Unión, así como del principio de subsidiariedad, los derechos que emanan, en particular, de las tradiciones constitucionales y las obligaciones internacionales comunes a los Estados miembros, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Unión y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos*»[399].

62. Es importante recordar esto porque los últimos atentados terroristas ocurridos en el territorio de la UE han generado una especie de "estado global de emergencia"[400], que, como decíamos, parece ir por el camino opuesto. La batalla frente el terrorismo ha conducido a la adopción individualizada de medidas extraordinarias que, aun siendo de diferente tenor y naturaleza, han llevado aparejadas serias limitaciones de los derechos fundamentales. Algunos gobiernos han introducido modificaciones en sus regímenes de excepción (estado

[396] CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2007/C 303/01), *Diario Oficial de la Unión Europea*, C 303 de 14/12/2007, págs. 1-16. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:ES:PDF [consulta: 13 de junio de 2015].

[397] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 28).

[398] Al respecto véase, Mónica ARENAS RAMIRO (2006: 208-211).

[399] CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2007/C 303/01). A través de la referencia al valor de la dignidad humana presente en el Preámbulo y la elección de consagrar su intangibilidad desde el principio, parte de la doctrina ha planteado la hipótesis de que existe en la Carta, en el sistema comunitario, la plena realización de un proceso de «*costituzionalizzazione della persona*». *Vid*. Carlo CASTRONOVO (2007), «La persona», en Carlo CASTRONOVO, Salvatore MAZZAMUTO (a cura di), *Manuale di diritto privato europeo*, Milano, Giuffrè, vol. 1, págs. 193-215.

[400] *Vid*. Rosario SERRA CRISTÓBAL (2014), «The Impact of Counter-terrorism Security Measures on Fundamental Rights: The Need for Supranational Common Standards of Rights Protection to respond to terrorism risk», en *IXth World Congress of Constitutional Law, "Constitutional Challenges: Global and Local"*, Oslo, 16 - 20 June 2014, pág. 18. En particular el autor usa el término «*global state of emergency*». También, véanse Lorena FORNI, Tiziana VETTOR (a cura di) (2018), *Sicurezza e libertà in tempi di terrorismo globale*, G. Giappichelli Editore, mayo, págs. 304.

de emergencia)[401] o en leyes antiterroristas, e incluso se han propuesto modificaciones de la Constitución (como en el caso de Francia). Y, sin embargo, en otros Estados europeos los remedios contra el terrorismo se han amparado en la normativa ya existente.

63. En este ámbito, el alcance de la confidencialidad de la información personal y de la protección de la privacidad personal, además de los Tratados, es especialmente reconocido en la Carta de Niza[402], en particular en los artículos 7 y 8 (*infra*). Sin embargo, es sólo con el Tratado de Lisboa en 2009 (*vid*. artículo 6, apartado 1 del TUE), con el fin de reforzar la protección de los mecanismos de las libertades personales, que la Carta ocupa en la Unión el más alto nivel, atribuyéndole el mismo valor jurídico que los Tratados constitutivos[403], por tanto, formando parte pues del Derecho originario de la Unión. Así, "los derechos, libertades, valores y principios establecidos en la CDFUE se convierten legalmente vinculantes para todos los Países de la UE que ratificaron el Tratado de 2009, confiriendo mejor claridad y seguridad jurídica a los ciudadanos de la UE". El resultado es una obligación directa, no sólo para el legislador europeo, sino también para el legislador nacional en la aplicación de las obligaciones comunitarias y, en este contexto, el Tribunal de Justicia que, como veremos más adelante[404], asume un papel importante como guardián de los derechos fundamentales.

64. La Carta de Niza, además de recoger los denominados "derechos clásicos", resultó innovadora, en particular porque incluye, entre otras cuestiones, la discapacidad, la edad y la orientación sexual como motivos de discriminación prohibidos, y establece como derechos fundamentales el acceso a los documentos, la buena administración y, como dicho, la protección de datos[405]. En particular, dentro del Título II de la Carta, dedicados a las

[401] *Amplius* Emanuele SOMMARIO (2018), *Stati d'emergenza e trattati a tutela dei diritti umani*, G. Giappichelli, págs. 316.
[402] CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2007/C 303/01). Tenga en cuenta cómo tuvo lugar la publicación de la Carta no en la serie "L" del Diario Oficial de la Unión Europea, propia de los actos normativos vinculantes, sino en la serie "C", reservado para los actos no vinculantes, o actos de los llamados derecho blando: la Carta, en una primera fase, tenía, de hecho, sólo un valor político.
[403] La Carta, como conocemos, no se inserta en el Tratado de Niza, quedando proclamada por el punto de vista político, pero no dotada con adecuada eficacia jurídica preceptiva. Su proclamación solemne no confirió a la Carta un carácter jurídicamente vinculante. Esta limitación, sin embargo, no impidió a este último influenciar ampliamente el desarrollo del sistema normativo comunitario y de los estados nacionales individuales. Hoy en día, este valor está en realidad reforzado. De hecho, el Tratado por el que se establece una Constitución para Europa recoge la Carta de los Derechos Fundamentales de la Unión Europea (parte II). TRATADO POR EL QUE SE ESTABLECE UNA CONSTITUCIÓN PARA EUROPA, Roma el 29 de octubre de 2004, *Diario Oficial de la Unión Europea*, C 310 de 16 de diciembre de 2004.
[404] *Cfr*. Capítulo IV.
[405] «La protección de los derechos fundamentales en la Unión Europea», en en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet:

libertades, se coloca el artículo 6 (Derecho a la libertad y a la seguridad), que reconoce que «*toda persona tiene derecho a la libertad y a la seguridad*»; el artículo 7 (Respeto de la vida privada y familiar), que establece que «*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*»[406]; y el artículo 8 (Protección de datos de carácter personal), que dispone que «*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente*»[407]. Dicho artículo establece que estos datos sean tratados de acuerdo con el principio de lealtad, para fines específicos y garantiza a cada persona "el derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación". También establece que el cumplimiento de este derecho está sujeto al control de una autoridad independiente. El artículo 47 de la Carta garantiza el derecho a la tutela judicial efectiva y el derecho a que su causa sea examinada de manera equitativa, pública y dentro de un plazo razonable (*vid*. más adelante).

65. Pese a estar basada en el CEDH y en otros instrumentos europeos e internacionales, en la Carta encontramos una diferencia sustancial con el CEDH. En este último sólo se reconoce el derecho a la vida privada (artículo 8 del CEDH), en cambio la Carta reconoce el derecho al respeto a la vida privada y familiar (artículo 7) y el derecho a la protección de datos personales (artículo 8); es decir, reconoce ambos derechos como independientes y

http://www.europarl.europa.eu/factsheets/es/sheet/146/la-proteccion-de-los-derechos-fundamentales-en-la-union-europea [consulta: 01 de junio de 2019].

406 «*Los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del CEDH. A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra "correspondencia" por la de "comunicaciones". De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que el artículo correspondiente del CEDH*». EXPLICACIONES SOBRE LA CARTA DE LOS DERECHOS FUNDAMENTALES (2007/C 303/02), *Diario Oficial de la Unión Europea*, C 303 de 14.12.2007, págs. 17–35. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32007X1214(01) [consulta: 18 de junio de 2015]. *Vid*. Alfonso ORTEGA GIMÉNEZ (2015: 44). El artículo 7 contiene cuatro garantías diferentes, como se expone en el comentario sobre la CDFUE: derecho al respeto de la vida privada, a la vida familiar, al domicilio y al secreto de las comunicaciones. Martin ARACELI MANGAS (2008: 209-222).

407 A diferencia de lo que sucede con otros derechos «*se opta por identificar lo que podría ser una suerte de contenido esencial del mismo: el principio de licitud, el principio de finalidad, el principio del consentimiento y del fundamento legal del tratamiento, el derecho de acceso y de rectificación. Incomprensiblemente, no se citan otros principios o derechos reconocidos comúnmente como parte integrante del estándar mínimo consagrado en todos los textos jurídicos europeos. No aparece el derecho de información, el principio de calidad, el derecho de cancelación o el principio de seguridad, por mencionar algunos. Tampoco se alude al régimen especial de los datos sensibles, por lo que tal vez hubiera sido más acertado limitarse a proclamar el derecho, sin aludir a las concretas facultades que lo integran*». *Vid*. María del Carmen GUERRERO PICÓ (2005).

autónomos[408]. En pocas palabras, el derecho al respeto de la vida privada y el derecho al tratamiento de datos personales se incluyen ahora en el derecho primario de la UE. Es decir, aparecen "constitucionalizados", en los artículos 7 y 8 de la CDFUE, y, en particular, como un derecho fundamental (artículo 8, apartado 2), sin embargo, independiente del derecho a la vida privada y familiar en virtud del artículo 7[409], lo que confirma, una vez más, la importancia que los Estados miembros de la Unión otorgan a la protección de la privacidad. La Carta eleva explícitamente el nivel de esta protección a la de un derecho fundamental en la legislación de la UE[410].

66. Entre las dos disposiciones legales, el artículo 8 de la Carta tiene una mayor capacidad de innovación, ya que introduce la autonomía del principio de la "protección de los datos personales" con respecto a la protección de la vida privada[411]. El artículo reconoce a todas las personas el derecho a la protección de los datos personales que le conciernen. La protección es, por lo tanto, limitada a las personas físicas de la misma manera querequiere la Directiva europea 95/46/CE y ahora el RGPD. El segundo apartado, relativo a las condiciones bajo las cuales es permisible el tratamiento de datos personales, simplemente establece que los datos deben ser tratados de acuerdo con el principio de lealtad y para fines concretos. El tratamiento de los datos se considera legítimo sólo en presencia del consentimiento de la persona afectada o de otra base establecida por la ley, lo que deja a la discreción del legislador la elección de los márgenes de derogación respecto al consentimiento de la persona afectada. Si se cumplen estas condiciones, no hay interferencia con el derecho a la protección de datos, aunque la recopilación, el almacenamiento o la divulgación de esos datos pueden todavía interferir con la vida privada y por lo tanto

[408] Otra literatura jurídica se ha basado en los regímenes diferenciales existentes en los ámbitos no cubiertos por la Directiva 95/46/CE, creyendo que la inclusión del derecho a la protección de datos personales en el catálogo de los derechos reconocidos por la Unión tenía el objetivo de extender la aplicación de los principios consagrado en la Directiva a todos tratamientos de datos personales, incluyendo los realizados en el contexto del segundo y tercer pilar. *Vid*. Antoinette ROUVROY, Yves POULLET (2009), «The Right to Informational Self Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy», en Serge GUTWIRTH and others (eds.), *Reinventing Data Protection?*, Springer Netherlands, pág. 71. Sin embargo, este objetivo no se ha realizado en la realidad práctica. Incluso los nuevos instrumentos jurídicos de 2016 han privilegiado el uso de dos instrumentos jurídicos diferentes (Reglamento y Directiva), lo que perpetúa el enfoque de "doble vía", por razones relativas a la especificidad del sector de cooperación policial y judicial. Orla LYNSKEY (2014: 4).

[409] El artículo 7 se encuentra un paso adelante de los demás textos protectores de los derechos fundamentales – en relación con la protección de datos personales – al reconocer la importancia del derecho a proteger la vida privada y familiar, mediante el respeto a las comunicaciones, que se realizan a través de la utilización de diversos medios.

[410] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[411] Martin ARACELI MANGAS (2008: 223-243).

requieren justificación[412]. Obviamente, en la mayoría de los casos, esta justificación debería ser fácil si se cumplen las condiciones del tratamiento autorizado. Sin embargo, se considera que la Carta establece, bajo las disposiciones de artículo 53[413], un nivel de protección al menos equivalente a la luz del Derecho comunitario. Igualmente, siempre en el segundo apartado del artículo 8 de la Carta, se menciona que toda persona tiene "el derecho de acceso y rectificación" de los datos recogidos que le conciernan. En la última parte de este artículo, se prevé que «*el respeto de estas normas quedará sujeto al control de una autoridad independiente*».

67. Las explicaciones que acompañan la Carta de Niza, en particular nos referimos a la explicación relativa al artículo 8[414], parecen restringir el alcance de la disposición de que se trate de una mera repetición del acervo. Sin embargo, el artículo 8 se presenta como centro de esta innovación iniciada por la Carta del que resulta evidente el carácter innovador de la norma[415]. Este novedoso derecho, se ha caracterizado por: a) la formalización del derecho a la protección de datos de carácter personal; y b) el paso de éste a formar parte del orden

[412] TEDH, *Amann contra Suiza* [GS], núm. 27798/95, sentencia de 16 de febrero de 2000, apartados 69 y 80; TEDH, *Rotaru contra Romania* [GS], núm. 28341/95, sentencia de 04 de mayo de 2000, apartado 46.

[413] Artículo 53 (Nivel de protección) de la CDFUE: «*Ninguna de las disposiciones de la presente Carta podrá interpretarse como limitativa o lesiva de los derechos humanos y libertades fundamentales reconocidos, en su respectivo ámbito de aplicación, por el Derecho de la Unión, el Derecho internacional y los convenios internacionales de los que son parte la Unión o todos los Estados miembros, y en particular el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como por las constituciones de los Estados miembros*»

[414] Su explicación oficial refleja una formulación lacónica y no ofrece ideas suficientemente clarificadoras a niveles exegéticos: «*Explicación relativa al artículo 8 - Protección de datos de carácter personal. Este artículo se ha basado en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31), así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El artículo 286 del Tratado CE ha sido sustituido por el artículo 16 del Tratado de Funcionamiento de la Unión Europea y el artículo 39 del Tratado de la Unión Europea. Conviene señalar asimismo el Reglamento (CE) n. 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1). La Directiva y el Reglamento mencionados establecen condiciones y límites para el ejercicio del derecho a la protección de los datos de carácter personal*». *Vid*. EXPLICACIONES SOBRE LA CARTA DE LOS DERECHOS FUNDAMENTALES (2007/C 303/02).

[415] Como se constata también en la jurisprudencia más reciente del TJUE. *Vid*. Capítulo IV de esta misma investigación. En doctrina *vid*. Marta CARTABIA (2007), «L'ora dei diritti fondamentali nell'Unione Europea», en Marta CARTABIA (a cura di), *I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Bologna, Il Mulino, págs. 31-35, pone de relieve cómo la Carta, bajo una "apariencia de codificación", introduce importantes novedades de contenido dentro de la gama de los derechos fundamentales y se encuentra entre las disposiciones más emblemáticas también el artículo 8. De hecho, como lo demuestra el Preámbulo, la Carta fue concebida con el objetivo de consolidar, a través de una fundación de derecho positivo, derechos preexistentes en el orden comunitario, pero terminó yendo más allá de la intención original en la identificación de los derechos destinados a ser consagrados por la labor de codificación. También *vid*. Juan Fernando LÓPEZ AGUILAR (2017: 558).

público europeo y de los derechos de sus ciudadanos. Éste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado de otros como el respeto a la vida privada y familiar. Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores. El reconocimiento de este derecho, autónomo y independiente del derecho a vida privada, «*se debe a la toma de conciencia necesaria para garantizar una tutela específica y efectiva frente a la recogida y almacenamiento de información sobre las personas, que han facilitado la posibilidad de crear bases de datos y de hacer circular la información contenida en ellas, dado su carácter potencialmente peligroso para algunos derechos fundamentales, y en especial, para la privacidad y los datos personales*»[416].

68. Por eso, la utilización de sistemas informáticos o automatizados para la gestión de la información y los flujos transfronterizos de datos personales requieren la elaboración de normas y prácticas compatibles que establecen normas mínimas de principios, derechos, obligaciones y seguridad en el ámbito de la protección de los datos personales[417]. Sin embargo, esto es extremadamente problemático, dado que, como unánimemente ha reconocido la doctrina, el derecho a la protección de datos personales difícilmente podría estar configurado de la misma manera que un principio general del Derecho comunitario, existiendo una tradición constitucional común en los Estados miembros y que carece de una referencia directa en el CEDH[418].

69. Este conflicto de definir el "equilibrio europeo" entre los derechos individuales a la protección de datos y las necesidades de seguridad de los Estados, si bien sigue formando parte de la división de competencias entre la Unión y los Estados miembros, se acentuará cada vez más debido a las numerosas leyes estatales aprobadas por los países en respuesta al número cada vez mayor de ataques terroristas en nuestras sociedades. Por ejemplo, Reino

[416] Alejandro Luis GACITÚA ESPÓSITO (2014: 166); Gloria GONZÁLEZ FUSTER (2014a: 190-191); GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999), Dictamen 4/99. Inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales, aprobado el 7 de septiembre de 1999. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26es.pdf [consulta: 12 de julio de 2015].

[417] Alejandro Luis GACITÚA ESPÓSITO (2014: 166). Este nuevo derecho fundamental establecido por la Carta de Niza no puede ser enmarcado en el esquema de "ser dejado solo", sino que se concreta en la atribución a cada uno del poder de "gobernar" la circulación de las informaciones que le conciernen. Se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y de la comunicación. La misma disposición, en su apartado 3, también determina un papel para-constitucional de la autoridad de control independiente para la protección de los datos personales. Así en Alfonso ORTEGA GIMÉNEZ (2015: 45).

[418] *Vid*. Gloria GONZÁLEZ FUSTER (2014a: 173-185); Orla LYNSKEY (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, págs. 89 y ss.

Unido, Francia, Alemania y, más recientemente, Italia han establecido programas de vigilancia digital para contrastar la amenaza terrorista antes de que ocurran los ataques[419]. Estas medidas utilizan tecnologías que requieren bases de datos digitales y, por lo tanto, la recopilación de datos electrónicos de los ciudadanos. Las "*laws of fear*" ("leyes del temor") en cuestión son competencia de los Estados y no están directamente sujetas a los artículos 7 y 8 de la Carta, como se aclara en el artículo 51 de la misma, ya que se dirigen a las instituciones, órganos y organismos de la Unión, mientras que los Estados miembros están obligados a respetarlas sólo cuando aplican el Derecho de la Unión[420]. Como consecuencia de la atribución de competencias, la protección de la intimidad y la seguridad de los ciudadanos está realmente confiada a la legislación nacional y no europea.

70. De la lectura de los artículos de la Carta que se han puesto de manifiesto, tenemos que aclarar y enfatizar el aspecto del real alcance que éstos tienen en los particulares[421]. Como sabemos, la legislación comunitaria en materia de protección de datos impone obligaciones similares en lo que respecta al tratamiento de la información personal de las autoridades públicas y de las partes privadas. Sin embargo, estas obligaciones no se derivan directamente de los artículos 7 y 8 de la Carta sino de la Directiva sobre protección de datos de 1995. Si bien los derechos fundamentales a la privacidad y la protección de datos establecidos en la Carta están enmarcados con suficiente apertura para permitir las obligaciones de las partes privadas, su contexto sugiere que sólo se dirigen a las autoridades públicas. De conformidad con el apartado 1 del artículo 51 de la Carta, sus disposiciones se dirigen a las instituciones, órganos y organismos de la Unión, así como a los Estados miembros cuando aplican la legislación de la UE. Por lo tanto, regula, en particular, el trabajo

[419] Para un análisis comparativo de las medidas legislativas relativas al terrorismo, *vid*. Laurent MAYALI and John YOO (2016), «A Comparative Examination of Counter-Terrorism Law and Policy», en J*ournal of Korean Law*, vol. 16, págs. 91-144. Disponible en Internet: https://ssrn.com/abstract=2949078 [consulta: 09 de mayo de 2017]. Con respecto a Italia, *vid*. Giovanna DE MINICO (2015), «Le libertà fondamentali in tempo di ordinario terrorismo», en *Federalismi.it*, núm. 10. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29517 [consulta: 25 de mayo de 2015].

[420] Artículo 51 (Ámbito de aplicación) de la CDFUE: «*1. Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión. 2. La presente Carta no amplía el ámbito de aplicación del Derecho de la Unión más allá de las competencias de la Unión, ni crea ninguna competencia o misión nuevas para la Unión, ni modifica las competencias y misiones definidas en los Tratados*».

[421] Sobre la eficacia vinculante de la CDFUE en las relaciones entre particulares (eficacia horizontal), *vid*. el trabajo de Juan Ignacio UGARTEMENDIA ECEIZABARRENA (2017), «La eficacia entre particulares de la Carta de Derechos Fundamentales de la Unión Europea a la luz de la jurisprudencia del Tribunal de Justicia», en *UNED. Teoría y Realidad Constitucional*, núm. 39, págs. 366 y ss. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19161 [consulta: 24 de julio de 2017].

legislativo y decisonal de la Comisión, del Parlamento y del Consejo, cuyas normas deben cumplir con la Carta. Con respecto a los Estados miembros, la misma afirma que «*se aplica sólo cuando ponen en práctica el Derecho de la Unión. No se aplica, por tanto, en las situaciones que no tengan ninguna relación con ésta. La fuerza jurídica vinculante conferida a la Carta por el Tratado de Lisboa no ha modificado esta situación, ya que este último especifica claramente que las disposiciones de la Carta no amplían, en modo alguno, las competencias de la Unión tal como quedan definidas en los Tratados*»[422].

71. El derecho a la vida privada y el derecho a la protección de datos tal y como figuran en la Carta, no crean directamente obligaciones a los particulares[423].

3.2. Limitaciones a la privacidad y a la protección de datos personales en virtud de la CDFUE

72. El derecho fundamental a la protección de datos personales en virtud del artículo 8 de la Carta, como dicho antes, "no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad"[424]. La Carta, de manera distinta del CEDH, no incluye la injerencia en los derechos garantizados, aunque incluye una disposición sobre las limitaciones del ejercicio de los derechos y libertades en ella reconocidos. El artículo 52, apartado 1, de la Carta reconoce así que "se pueden imponer limitaciones al ejercicio de derechos tales como los establecidos en los artículos 7 y 8 de la Carta". La aplicación de estas limitaciones generales de los derechos fundamentales de la Carta a la protección de datos plantea cuestiones interesantes. De conformidad con el artículo 52 (Alcance de los derechos garantizados), apartado 1, «*Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y*

[422] Alejandro Luis GACITÚA ESPÓSITO (2014: 164-165).

[423] Para el CEDH, la situación es aún más clara, ya que, en virtud del artículo 1, las Partes Contratantes, y no las personas, son responsables. Sin embargo, el TEDH ha reconocido que las obligaciones positivas de estos Estados son inherentes al respeto efectivo de ciertos derechos del Convenio, en particular en lo que concierne al respeto de la vida privada, y que estas obligaciones pueden comportar la adopción de medidas destinadas a garantizar el respeto a la privacidad incluso en el ámbito de las relaciones de los individuos entre sí. *Vid*. Juliane KOKOTT and Christoph SOBOTTA (2013), «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», en *International Data Privacy Law*, vol. 3, núm. 4. Disponible en Internet: https://academic.oup.com/idpl/article/3/4/222/727206/The-distinction-between-privacy-and-data [consulta: 16 de julio de 2015]. Juan Ignacio UGARTEMENDIA ECEIZABARRENA (2017: 366 y ss.).

[424] *Vid*. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 37). Sobre la protección de datos personales como derecho fundamental, véanse la investigacion de Pablo Pascual HUERTA (2017), *La génesis del derecho fundamental a la protección de datos personales*, Tesis Doctoral, Madrid, Universidad Complutense de Madrid Facultad de Derecho Departamento de Derecho Constitucional, págs. 369.

respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás». El derecho a la protección de datos personales, como los otros derechos contemplados por la Carta, que constituye disposiciones de los Tratados se ejercerá «*en las condiciones y dentro de los límites determinados por éstos*» (apartado 2).

73. A pesar de la distinta redacción, las condiciones del tratamiento lícito del artículo 52, apartado 1, de la Carta evocan las contempladas en el artículo 8, apartado 2, del CEDH (*cfr*. *supra*), que protege la protección de datos como parte del derecho más amplio al respeto de la vida privada y familiar[425]. Entonces, el artículo 52, apartado 1, regula el alcance de los derechos garantizados en los artículos 7 y 8 de la Carta, señala que «*cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser*»: 1) «*establecida por ley y respetar el contenido esencial de dichos derechos y libertades*». Este requisito implica que las limitaciones deben basarse en una base legal que sea adecuadamente accesible y previsible, y que se formule con suficiente precisión para permitir a los individuos comprender sus obligaciones y regular su conducta. La base legal también debe definir claramente el alcance y la forma del ejercicio del poder por parte de las autoridades competentes para proteger a las personas contra la interferencia arbitraria. Cualquier limitación de los derechos fundamentales protegidos por la Carta debe respetar la esencia de esos derechos. Esto significa que las limitaciones que son tan extensas e invasivas como para privar un derecho fundamental de su contenido básico no pueden justificarse. Si la esencia del derecho se ve comprometida, la limitación debe considerarse ilegal, sin necesidad de evaluar si cumple un objetivo de interés general y satisface los criterios de necesidad y proporcionalidad; 2) respetar el "principio de proporcionalidad". Significa que las ventajas resultantes de la limitación deben superar las desventajas de esta última causa en el ejercicio de los derechos fundamentales en juego. Para reducir las desventajas y los riesgos para el disfrute de los derechos a la privacidad y la protección de datos, es importante que las limitaciones contengan garantías adecuadas; 3) necesaria. Puede ser necesaria una limitación si es necesario adoptar medidas para el objetivo de interés público perseguido, pero la necesidad, tal como lo interpreta el TJUE, también implica que las medidas adoptadas deben ser menos invasivas en comparación con otras opciones para lograr el mismo objetivo. En cuanto a las limitaciones del derecho al respeto de la vida privada y la protección de datos personales, el TJUE aplica una prueba estricta de necesidad, sosteniendo que las excepciones

[425] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 73).

y limitaciones deben aplicarse únicamente en la medida estrictamente necesaria. Si se considera que una limitación es estrictamente necesaria, también es necesario evaluar si es proporcionada; y 4) responda «*efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás*» (artículo 52, apartado 1). En cuanto a los objetivos de interés general, éstos incluyen los objetivos generales de la UE afirmados en el artículo 3 del TUE[426]. Con respecto a la exigencia de proteger los derechos y libertades de las personas, "el derecho a la protección de los datos personales a menudo interactúa con otros derechos fundamentales"[427].

74. Cuando la protección de datos interactúa con otros derechos, tanto el TEDH como el TJUE han declarado repetidamente que es necesario un ejercicio de equilibrio con otros derechos al aplicar e interpretar el artículo 8 del CEDH y el artículo 8 de la Carta. Además del ejercicio de equilibrio llevado a cabo por estos tribunales, los Estados pueden, si es necesario, adoptar una legislación "para armonizar el derecho a la protección de datos personales con otros derechos". Por este motivo, el RGPD especifica más el artículo 52, apartado 1, de la Carta a este respecto: el artículo 23, apartado 1, del Reglamento enumera una serie de objetivos de interés general considerados legítimos para limitar los derechos de las personas, siempre que la limitación respete la esencia del derecho a la protección de datos personales y sea necesario y proporcionado: la seguridad nacional del Estado; «*la defensa; la seguridad pública; la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; otros objetivos importantes de interés público general de la Unión o de un Estado miembro* (…)».

---

[426] Artículo 3 (antiguo artículo 2 TUE) del TUE: «*1. La Unión tiene como finalidad promover la paz, sus valores y el bienestar de sus pueblos. 2. La Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia. 3. La Unión establecerá un mercado interior. Obrará en pro del desarrollo sostenible de Europa basado en un crecimiento económico equilibrado y en la estabilidad de los precios, en una economía social de mercado altamente competitiva, tendente al pleno empleo y al progreso social, y en un nivel elevado de protección y mejora de la calidad del medio ambiente. Asimismo, promoverá el progreso científico y técnico. La Unión combatirá la exclusión social y la discriminación y fomentará la justicia y la protección sociales, la igualdad entre mujeres y hombres, la solidaridad entre las generaciones y la protección de los derechos del niño. La Unión fomentará la cohesión económica, social y territorial y la solidaridad entre los Estados miembros. La Unión respetará la riqueza de su diversidad cultural y lingüística y velará por la conservación y el desarrollo del patrimonio cultural europeo*. (…)».

[427] En este sentido, *vid*. Ilenia ITALIANO (2015), *La protezione dei dati personali e il bilanciamento con altri diritti personali nel Diritto dell'Unione Europea*, Tesis Doctoral, Roma, Università degli Studi Roma Tre Scuola Dottorale Internazionale "Tullio Ascarelli" Diritto - Economia - Storia, Sezione "diritto europeo su base storico comparatistica", XVII° Ciclo, págs. 152.

75. Se trata de la aplicación de la jurisprudencia del TEDH y del Tribunal de Justicia de la UE[428]: cuando se han pronunciado sobre la posibilidad de los Estados de restringir el derecho a la vida privada y familiar de conformidad con el apartado 2 del artículo 8 del CEDH, han tratado de limitar este derecho reconocido a los Estados con el fin de no dejar sin sentido el mismo derecho. En este contexto, como se recordará, el TEDH ha afirmado en repetidas ocasiones que la interferencia tiene que ser basada en "una necesidad social imperiosa y tiene que ser proporcionada" al objetivo perseguido, determinada en la legislación nacional con las garantías adecuadas y suficientes para evitar el riesgo de abusos, y que el proceso de toma de decisiones que lleva a la adopción de medidas de injerencia sea justo y respete oportunamente los intereses individuales protegidos por el artículo 8[429].

76. ¿Pueden estas limitaciones justificar el trato ilegal de datos personales o el procesamiento para fines que no están cubiertos por el fundamento jurídico de su recogida? Como la protección de datos personales es un derecho fundamental distinto e independiente en el ordenamiento jurídico de la UE, protegido por el artículo 8 de la Carta, cualquier tratamiento de datos personales por sí mismo constituye una interferencia con este derecho. Es irrelevante si los datos personales en cuestión se relacionan con la vida privada de una persona o son datos sensibles. Para ser legal, la injerencia debe cumplir con todas las condiciones enumeradas en el artículo 52, apartado 1, de la Carta.

77. Por lo tanto, hay espacio para aplicar las limitaciones generales a la protección de datos, aunque bajo algunas condiciones. Sin embargo, al aplicar estas limitaciones generales, deben tenerse en cuenta los riesgos específicos asociados con el tratamiento de datos personales. A este respecto, el TEDH explicó que cuanto mayor sea la cantidad y la sensibilidad de los datos almacenados y disponibles para su divulgación, más importante será el contenido de las salvaguardias que se deben aplicar en las diversas etapas cruciales del tratamiento ulterior de los datos[430]. Por consiguiente, una referencia general a la

[428] *Vid*. Capítulo IV *infra*.

[429] *Amplius*, Daniel I. GARCÍA SAN JOSÉ (2001: 67-89); Elena VARANI (2005), *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario. Dalla Carta dei diritti fondamentali dell'Unione Europea al decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"*, págs. 20-21. Disponible en Internet: https://uonted.files.wordpress.com/2008/02/varaniprivacy.pdf [consulta: 04 de agosto de 2017]; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 40).

[430] *Vid*. Charles BOURNE (2012), «Retention and disclosure of police caution data infringe Article 8», en *The UK Human Rights Blog*. Disponible en Internet: https://ukhumanrightsblog.com/2012/11/15/retention-and-disclosure-of-police-caution-data-infringe-article-8-charles-bourne/ [consulta: 21 de julio de 2015]; James B. JACOBS, Elena LARRAURI (2015), «Disclosure of nonconviction records may violate European Convention on Human Rights», en *Collateral Consequences Resource Center*. Disponible en Internet: http://ccresourcecenter.org/2015/01/30/criminal-record-privacy-according-european-court-human-rights/ [consulta: 21 de julio de 2015].

seguridad pública no es suficiente para justificar limitaciones a la protección de datos. Las limitaciones deben ser claramente definidas, necesarias y proporcionadas. Por su parte, el Tribunal de Justicia ha abordado algunas de estas cuestiones otorgando una protección al individuo frente a intromisiones ilegítimas de los poderes públicos a través de grabaciones, mecanismos de escuchas u otros medios técnicos[431]. La finalidad es proteger a toda persona europea de las intromisiones de los poderes públicos en su esfera íntima y privada, como sucede en los casos más recientes explicados en la introducción, escuchas telefónicas, vulneraciones cometidas en Internet y el desarrollo del comercio electrónico.

78. No obstante, existe una garantía asociada a la protección de datos cuando una limitación parece muy difícil de justificar: el control del cumplimiento por una autoridad independiente, tal como se prevé en el apartado 3 del artículo 8 de la Carta[432]. Por supuesto, puede haber problemas de seguridad asociados con ciertos casos de tratamiento de datos, por ejemplo, si están relacionados con la investigación de terrorismo o espionaje. En estos casos, el acceso necesario de las autoridades independientes plantea el riesgo de que se divulguen datos confidenciales. Sin embargo, incluso en tales casos debería ser posible identificar a las personas a las que se pueda confiar el control independiente de la protección de datos y el mantenimiento de la confidencialidad al mismo tiempo[433]. La creación, a escala comunitaria, de un «*control de una autoridad independiente*», previsto ya por el artículo 286 del TCE, ha tenido lugar con el Reglamento (CE) n. 45/2001[434], que estableció el Supervisor Europeo de Protección de Datos (en adelante, SEPD). Paralelamente, "los Estados miembros dispondrán que una o más autoridades públicas independientes se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación del nuevo RGPD"[435].

---

[431] *Vid*. TJUE (Sala Tercera), *Institut professionnel des agents immobiliers (IPI) contra Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte*, asunto C-473/12, sentencia de 7 de noviembre de 2013. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/index-ides-idphp.php [consulta: 04 de agosto de 2017].

[432] El Tribunal de Justicia ha subrayado repetidamente la importancia de esta independencia: TJUE (Gran Sala), *Comisión Europea contra República Federal de Alemania*, asunto C-518/07, sentencia de 9 de marzo de 2010; TJUE (Gran Sala), *Comisión Europea contra República de Austria*, asunto C-614/10, sentencia de 16 de octubre de 2012.

[433] Las Autoridades Supervisoras de la OLAF y de Europol pueden servir de ejemplo.

[434] REGLAMENTO (CE) N. 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, *Diario Oficial de la Unión Europea*, L 8 de 12.1.2001, págs. 1–22. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32001R0045 [consulta: 25 de julio de 2015]. Este Reglamento ha sido derogado por el nuevo REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. 45/2001 y la Decisión n. 1247/2002/CE, *Diario Oficial de la Unión Europea*, L 295/39, 21.11.2018.

[435] *Vid*. *infra* artículos 51 y ss. del RGPD.

79. La Carta tiene la importancia de establecer el principio de regulación independiente en la materia, y no concentrar todos los poderes de vigilancia en una sola autoridad. Esta interpretación se ve confirmada por la jurisprudencia que, aunque el artículo 8, apartado 3 de la Carta se refiera genéricamente a la potestad de control de una autoridad independiente, pone de relieve la necesidad de que los poderes de vigilancia han de ser confiados a autoridades independientes, cuya institución en los Estados miembros constituye un "elemento esencial" de tutela de la protección de las personas con respecto al tratamiento de datos personales[436]. Por lo tanto, la legislación europea, como hemos tenido modo de señalar, "exige un control independiente como un mecanismo importante para garantizar una protección de datos efectiva". Las autoridades de control independientes son el primer punto de contacto para los interesados en casos de violaciones de la privacidad. Según la legislación de la UE y la legislación del CdE, el establecimiento de las autoridades de supervisión es obligatorio[437]. Ambos marcos legales describen las tareas y poderes de estas autoridades de manera similar a las incluidas en el RGPD. En principio, las autoridades de supervisión deberían, por lo tanto, funcionar de la misma manera en virtud de la legislación de la UE y del Consejo de Europa.

80. La Carta ha producido, sin embargo, otra consecuencia importante, relacionada con el hecho de que, al recordar el CEDH, constituye una cláusula de equivalencia, según la cual, «*en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no impide que el Derecho de la Unión conceda una protección más extensa*» (artículo 52, apartado 3). En el contexto de la comparación entre el artículo 8, apartado 2, del CEDH y artículo 52, apartado 3, frase primera, lo anterior únicamente puede significar que las condiciones para las injerencias justificadas con arreglo al artículo 8, apartado 2, del CEDH constituyen los requisitos mínimos para las limitaciones lícitas del derecho a la protección de datos con arreglo a la Carta. Por consiguiente, el tratamiento lícito de datos personales exige que, según lo que establece el artículo 52, apartado 3 de la Carta, en la medida en que ambos documentos contengan derechos correspondientes, el significado y el alcance de los derechos establecidos en la Carta sean los mismos que los establecidos en el Convenio. No obstante, esta disposición no impedirá

[436] *Vid*. TJUE (Gran Sala), *Comisión Europea contra República Federal de Alemania*, apartado 23; TJUE (Gran Sala), *Comisión Europea contra República de Austria*, apartado 37.
[437] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

que el Derecho de la Unión ofrezca una protección más amplia[438]. En consecuencia, el Convenio define la norma mínima que debe garantizarse también en la aplicación de la Carta.

81. Con el comienzo de la eficacia del Tratado de Lisboa en el diciembre de 2009, como comentamos, la Carta pasó a ser jurídicamente vinculante para las instituciones de la UE y los Estados miembros cuando apliquen el Derecho de la UE[439]. Por consiguiente, «*la Carta forma parte del derecho primario de la Unión y, como tal, sirve de parámetro de referencia a la hora de examinar la validez del Derecho derivado y de las medidas nacionales*»[440].

82. Ahora, aunque la Carta de Niza no forma parte del Tratado de Lisboa, según el artículo 6, apartado 1, del TUE, «*la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea,* (…) *la cual tendrá el mismo valor jurídico que los Tratados*» (TUE y TFUE). De esta forma, con el comienzo de la eficacia del Tratado de Lisboa, la Carta se liberó del *status* de «*limbo*» jurídico[441], en el que había sido relegada «*en letargo*»[442] y ha podido comenzar a desplegar todo su potencial expansivo, constituyendo el *iter* final y esencial que llevó a reconocer la privacidad, y en particular la protección de los datos personales, como un derecho fundamental de la persona en el sistema legal europeo.

83. También hay que recordar que la Carta, como fuente primaria de la protección de los derechos fundamentales en la UE, se convierte en parámetro de la legalidad de los actos de la Unión. La integración entre la legislación europea y nacional es tal que los derechos en la Carta influyen en las decisiones políticas y legislativas, y con frecuencia lo hacen de manera bastante sustancial. Esto es aún más cierto debido a la interpretación de los Tratados por parte del Tribunal de Justicia, que extendió por mucho tiempo el ámbito de aplicación de los

[438] EXPLICACIONES SOBRE LA CARTA DE LOS DERECHOS FUNDAMENTALES (2007/C 303/02), *cfr. Explicación relativa al artículo 8 - Protección de datos de carácter personal y Explicación relativa al artículo 52 - Alcance e interpretación de los derechos y principios.*

[439] COMISIÓN EUROPEA - Comunicado de prensa (2010), La Comisión Europea adopta una estrategia para garantizar el respecto de la Carta de los Derechos Fundamentales de la UE, IP/10/1348, Bruselas, 19 de octubre de 2010. Disponible en Internet: http://europa.eu/rapid/press-release_IP-10-1348_es.htm [consulta: 29 de julio de 2015].

[440] Sarah SY (2017b), «La Carta de los Derechos Fundamentales de la Unión Europea», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_1.1.6.html [consulta: 04 de agosto de 2017].

[441] En Marta CARTABIA (2011), «I 'nuovi' diritti», en *Atti del Convegno del CESEN "Diritto della Unione Europea e status delle confessioni religiose"*, Roma, Istituto L. Sturzo, 8-9 ottobre 2010, págs. 5 y ss.

[442] Pedro CRUZ VILLALÓN (2017), «El valor de posición de la carta de derechos fundamentales en la comunión constitucional europea», en *UNED. Teoría y Realidad Constitucional*, núm. 39, pág. 92. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19146 [consulta: 14 de julio de 2017].

derechos fundamentales que interpreta, identificando las implicaciones en los Estados miembros y vinculando incluso a los organismos e instituciones nacionales[443]. Por lo tanto, las decisiones de los jueces en Luxemburgo proporcionan una perspectiva esencial para comprender la esfera y el alcance reales de la legislación europea sobre privacidad en donde las leyes estatales o europeas entran en conflicto con las disposiciones de los artículos 7 y 8 de la Carta.

84. Un ejemplo reciente de la reconciliación entre los derechos fundamentales se encuentra en la jurisprudencia común sobre la protección de datos de carácter personal, que ha tenido un importante impulso, como veremos, sobre todo desde el 2014 a 2016. A pesar de que realmente no falten también en tal ámbito intervenciones del Tribunal de Justicia de la Unión Europea también en los años anteriores, este último fue llamado repetidamente a pronunciarse sobre el valor del derecho de las personas a la protección de los datos personales[444], en concurso con otros derechos fundamentales (derecho de autor, la iniciativa económica, libertad de información y de expresión, la seguridad pública), en las relaciones entre personas físicas y jurídicas, así como entre los ciudadanos y los poderes públicos. Se trata de un intento de definir el equilibrio europeo entre los derechos individuales a la protección de datos y las necesidades de seguridad de los Estados.

85. A pesar de la división de la protección de la privacidad y de los datos personales en dos artículos específicos (artículos 7 y 8 de la Carta) con respecto al artículo 8 del CEDH, estas disposiciones legislativas han permitido décadas de jurisprudencia del TEDH en la materia, que ha interpretado el texto escrito en 1950, adaptándolo a nuestra cambiante sociedad. Y, en efecto, sobre esta base jurídica el ejecutivo europeo[445], indicando con precisión la necesidad de modernizar la legislación vigente a la luz de los "rápidos avances

[443] Raffaele BIFULCO, Marta CARTABIA, Alfonso CELOTTO (a cura di) (2001: 347).

[444] Como vamos a comprobar, el Tribunal de Justicia de la UE, ha reconocido a la Carta una valencia interpretativa de los derechos fundamentales sobre cuáles son los principios comunes de los sistemas jurídicos europeos. Por tanto, es un instrumento de la exégesis de las tradiciones constitucionales comunes a los Países europeos y de los jueces del Tribunal de Justicia y a los mismos jueces nacionales que aplican las leyes nacionales. Un ejemplo de ese nuevo papel interpretativo lo encontramos en la sentencia del Tribunal de Justicia de 8 de abril de 2014, *Digital Rights Ireland Ltd*, que en su papel de intérprete de los derechos humanos ha declarado nula la Directiva sobre conservación de datos, ya que es incompatible con la Carta de la UE. Véase Capítulo IV de esta investigación.

[445] La importancia ya incontestable del derecho a la protección de los datos personales por el sistema de la Unión, tal como subrayó el hecho de la reforma del marco jurídico, que se llevó a cabo con la aprobación del Reglamento general de protección de datos 2016/679, también para las relaciones con terceros estados ha sido puesta entre las prioridades de la nueva Comisión Europea presidida por el presidente Juncker. ESTADO DE LA UNIÓN 2016, Jean-Claude Juncker, presidente de la Comisión Europea, 14 de septiembre de 2016, pág. 10. Disponible en Internet: https://publications.europa.eu/es/publication-detail/-/publication/c9ff4ff6-9a81-11e6-9bca-01aa75ed71a1 [consulta: 09 de agosto de 2017].

tecnológicos y la globalización", propuso en 2012 el conocido paquete de reformas, basado en una propuesta de Reglamento sobre la protección de datos destinada a sustituir a la Directiva 95/46/CE, y una Directiva sobre protección de datos en el ámbito de la cooperación judicial y policial en materia penal, que sustituirá a la Decisión Marco 2008/977/JAI (*vid*. *infra*).

86. En fin, el reconocimiento del derecho a la protección de datos personales en la CDFUE es la culminación de una larga y compleja evolución normativa que tuvo su comienzo con la promulgación de la Directiva 95/46/CE y que ha dado lugar a un verdadero modelo europeo, que ahora se destaca claramente de los EE.UU.[446].

4. La aproximación fallida de los instrumentos legislativos vigentes en la Unión en materia de protección de datos

87. Los textos de los Tratados constitutivos de las Comunidades Europeas, nacidos con el objetivo de crear una integración económica entre los Estados, no incluyeron ninguna disposición para la protección de los derechos fundamentales. En el ordenamiento jurídico europeo, centrado inicialmente en la protección de las libertades económicas, dicha protección se ha desarrollado gradualmente en un sistema de protección de los derechos fundamentales gracias a la labor del Tribunal de Justicia (sobre este último asunto, nos remitimos al Capítulo dedicado).

88. Una de las primeras cuestiones que surgen en el marco de la integración europea que afectan a los derechos fundamentales concierne a los datos personales. Por lo tanto, en la década de los noventa se incorpora un elemento fundamental al debate: la construcción europea, que requiere ineludiblemente la constitución del mercado interior y exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales, sobre todo en el marco de una economía cada vez más globalizada y transfronteriza[447]. Este hecho ha madurado progresivamente la

[446] David COLE and Federico FABBRINI (2015), «Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders», en *Forthcoming in International Journal of Constitutional Law; iCourts Working Paper Series n. 33*. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657514 [consulta: 18 de julio de 2017].
[447] José Luis PIÑAR MAÑAS (2003), «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», en *Cuadernos de Derecho Público*, núms. 19-20, mayo-diciembre, pág. 48.

conciencia de los riesgos potenciales que el tratamiento de los datos podría tener sobre la privacidad de los individuos.

89. La armonización "mínima", perseguida por el Convenio n. 108, que contenía cláusulas elásticas y ofrecía amplio margen de discrecionalidad a los Estados, se consideró insuficiente para garantizar la plena protección, y las instituciones comunitarias advirtieron la necesidad de intervenir directamente en el campo para asegurar la adopción de un enfoque único[448], ya que la protección de los datos personales en Europa estaba regulada por leyes nacionales individuales no armonizadas[449]. La necesidad de un marco regulador único era más urgente para eliminar estos obstáculos.

90. Estos son los temas políticos y jurídicos subyacentes a la Directiva 95/46/CE, que dicta las líneas generales de la legislación sobre protección de datos personales. La Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, hasta mayo de 2018, fue el principal instrumento normativo en materia de protección de los datos personales en la Unión. Precisamente a causa de su peculiar génesis, la Directiva tenía una "doble personalidad", con el objetivo de conciliar dos propósitos distintos: "facilitar la libre circulación de datos personales en el mercado único y «*proteger los derechos fundamentales*» y «libertades de las personas», especialmente «*el derecho a la intimidad, en lo que respecta al tratamiento de datos personales*». La Directiva establecía unas «*condiciones generales para la licitud del tratamiento de datos personales*» y define los derechos de los interesados, al tiempo que prevé la designación de autoridades nacionales de control independientes.

91. Como consecuencia de la antigua estructura de pilares, la Directiva representaba un marco general (*lex generalis*) complementado con instrumentos normativos específicos (*lex specialis*). De forma complementaria a la Directiva de 1995, están en vigor diferentes instrumentos legislativos específicos[450], entre los que figuran instrumentos pertenecientes al

[448] David I. BAINBRIDGE, Nick PLATTEN (1996: 23).

[449] Aunque todos fueron inspirados por los principios fundamentales establecidos por el Convenio n. 108, aprobado en 1981 por el Consejo de Europa, las leyes nacionales eran muy diferentes en el contenido y afectaban negativamente a la competitividad y el buen funcionamiento del mercado único europeo.

[450] A nivel del derecho comunitario, la conservación y uso de los datos por fines de contraste de los delitos han sido abordadas por primera vez por la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Por ejemplo, esta Directiva reconocía, en su artículo 14 (Extensión del ámbito de aplicación de determinadas disposiciones de la Directiva 95/46/CE), que: «*Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y derechos*

antiguo primer pilar, como los siguientes: 1) la Directiva 2002/58/CE (modificada en 2009) sobre la privacidad y las comunicaciones electrónicas (también denominada Directiva *e-Privacy*); 2) la Directiva 2006/24/CE sobre la conservación de datos[451] (declarada inválida por el TJUE el 8 de abril de 2014, *vid*. Capítulo IV *infra*); 3) el Reglamento (CE) n. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre el año 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (derogada por el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. 45/2001 y la Decisión n. 1247/2002/CE)[452]; así como 4) instrumentos pertenecientes al antiguo tercer pilar, como la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (sustituida por la Directiva sobre protección de datos en el ámbito penal en mayo de 2018).

92. Desde estas primeras consideraciones, podemos deducir que no existía un marco jurídico unificado de protección de datos en el ámbito del ELSJ. De hecho, muchos de los intercambios de datos llevados a cabo por los cuerpos de seguridad de los Estados miembros se encontraban aún sujetos exclusivamente a leyes penales nacionales. Como veremos, según el *ex* artículo 3, apartado 2, de la Directiva 95/46/CE, las leyes europeas de protección de

(…) *cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicación* (…)». También véase el considerando 12 de la misma Directiva: «(…) *corresponde a los Estados miembros adoptar las medidas que consideren necesarias para la protección de la defensa de la seguridad pública, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal; que la presente Directiva no afectará a la capacidad de los Estados miembros a interceptar legalmente las telecomunicaciones para cualquiera de estos fines*». DIRECTIVA 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, *Diario Oficial de la Unión Europea*, L 024 de 30/01/1998, págs. 1–8. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31997L0066 [consulta: 02 de agosto de 2015].

[451] Después del 11-S, el equilibrio entre la privacidad y la seguridad se ha puesto en peligro. Precisamente con el fin de crear un sistema de salvaguardias y protecciones para el individuo en el mundo de las comunicaciones electrónicas, se habían puesto en marcha dos importantes directivas: la Directiva 2002/58/CE y la Directiva 2006/24/CE. Por ejemplo, en diciembre de 2001, el Parlamento Inglés aprobó la *Anti-terrorism, Crime and Security Act 2001*, que prevé la introducción de una serie de medidas estrictas en materia de controles, de detención de policía y las garantías judiciales de los sospechosos. *Vid*. Anti-terrorism, Crime and Security Act 2001, 14th December 2001. Disponible en Internet: http://www.legislation.gov.uk/ukpga/2001/24 [consulta: 12 de agosto de 2015].

[452] *Vid*. *supra*.

datos no son de aplicación en aquellos casos en los que el tratamiento de datos tenga un fin de «*seguridad pública, defensa, seguridad del Estado y actividades del Estado*» en el ámbito penal. Esta disposición se convirtió en un obstáculo cada vez que la UE ha intentado incorporar un nuevo instrumento de intercambio de datos en el campo de la seguridad pública.

93. La Decisión Marco de 2008[453] regulaba la protección de datos con arreglo al antiguo tercer pilar. Se trata de un ámbito no contemplado en la Directiva 95/46/CE (*ex* artículo 3, apartado 2), que se aplica al tratamiento de datos personales en el marco del antiguo primer pilar. La Decisión Marco sólo se aplicaba a los datos policiales y judiciales intercambiados entre Estados miembros, autoridades y sistemas conexos de la Unión, sin que se incluyan los datos nacionales[454].

94. Los apartados que ahora vamos a desplegar explican brevemente los conceptos jurídicos esenciales de algunos de los instrumentos legislativos vigentes en la Unión en materia de protección de datos; es decir, los objetivos, principios y límites de las normativas, teniendo bien presente el objeto de nuestra investigación. Aunque si, como se ha repetido repetidamente, la Directiva de 1995 y la Decisión Marco de 2008 han sido sustituidas por la nueva reforma, parece correcto hacer hincapié de algunos elementos distintivos de una normativa fundamental, especialmente en lo que respecta a nuestra investigación, con el fin de obtener una cuadro más completo sobre todo el tema. También porque algunos aspectos que estaban presentes en la Directiva y en la Decisión se han vuelto a proponer en la nueva legislación. En particular, nos centraremos en el análisis de la Directiva 95/46/CE y de la Decisión Marco 2008/977/JAI; por cuanto concierne a un igualmente importante acto normativo, la Directiva 2006/24/CE sobre la conservación de datos se analizará en el Capítulo dedicado al Tribunal de Justicia de la UE, ya que nos ayudará para entender las motivaciones que llevaron al Tribunal a declararla nula.

[453] Antes de 2008 la única solución era enmascarar este tipo de medidas bajo el paraguas del antiguo primer pilar, tal y como ocurrió con el acuerdo internacional para la recogida de datos de pasajeros entre las Comunidades Europeas y Estados Unidos en 2004, o la Directiva de conservación de datos adoptada en 2006.
[454] Aunque tal instrumento mejoró la situación de aquel momento, lo cierto es que la Decisión Marco 2008/977/JAI fue objeto de muchas críticas por ser demasiado ambigua y dejar un margen de discreción muy amplio para la implementación de los Estados miembros (*vid*. *infra*).

4.1. Los alcances limitados de la Directiva 95/46/CE relativa al tratamiento de los datos personales y su libertad de circulación

95. En el 18 de julio de 1990, la Comisión presenta al Consejo la primera propuesta de Directiva, el COM (90) 314-SYN 287 y 288, de 24/09/1990[455]. Después de un largo y difícil período de negociación - que se extendió durante cinco años[456] -, en 1995 fue aprobada la Directiva 95/46/CE que ha trazado los principios básicos de la "protección de las personas físicas con respeto al tratamiento de datos personales, además de la libre circulación de estos datos"[457], con el fin de armonizar la legislación interna relativa a «*la protección de las personas respecto del tratamiento*» y «*la libre circulación de datos personales*»[458]. Representa un importante paso adelante en comparación con el Convenio de Estrasburgo de 1981[459]: en efecto, "hace una operación de balance entre el mantenimiento de un nivel mínimo de protección y el respeto del principio europeo de libre circulación de datos personales".

96. La Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995[460] (en inglés, *Data Protection Directive*), hasta el inicio de la aplicación del nuevo Reglamento (UE) 2016/679[461], fue el «*principal instrumento jurídico de la UE en materia*

[455] En Álvaro A. SÁNCHEZ BRAVO (1998), *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, pág. 148; Ana Isabel HERRÁN ORTIZ (2002), *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Madrid, Editorial Dykinson, pág. 119.

[456] Hay que recordar también, que, en ese período, la situación política tiene un cambio importante y sustancial. Se produce la firma del Tratado de Maastricht el 7 de febrero de 1992, que modificó el Acta Única Europea vigente desde 1986.

[457] En el año 1992, COM (92) 442 Final, DOC n. 311, de 27 de noviembre de 1992, se inicia la tramitación del proyecto de Directiva de protección de datos que finalmente es aprobada como Directiva 95/46/CE. Ana Isabel HERRÁN ORTIZ (2002: 116 y ss.).

[458] Considerando 23 y artículo 1 de la DIRECTIVA 95/46/CE. Cuando se dictó la Directiva en el año 1995 no existía el reconocimiento de la protección de datos como tal en la Comunidad, por lo que no había competencias para legislar sobre una temática que no formaba parte de las políticas de la Unión, no estaba reconocida como derecho fundamental y tampoco aparecía en los Tratados constitutivos. Pero la visión de la importancia de la regulación del tratamiento de datos personales estaba constatada y de hecho se creó una Unidad de Protección de Datos, si bien inicialmente formaba parte de la Dirección General de Mercado Interior (por ello el nombre de la Directiva habla de "circulación de datos", para que de este modo tuviera encaje en el Derecho de la Unión). Posteriormente, en el año 2004 se trasladó a la Dirección General de Justicia, siendo el Jefe de Unidad en aquel momento Philippe Renaudière, actual Data Protection Officer (DPO) de la Comisión Europea. En María Belén SÁNCHEZ GONZÁLEZ (2016: 78).

[459] La Directiva se basó en las Directrices de la OCDE, en los principios del Convenio n. 108 y en las Directrices de las Naciones Unidas, pero los especificó y añadió nuevos elementos.

[460] En DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial de la Unión Europea*, L 281 de 23.11.1995, págs. 31–50. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046 [consulta: 16 de julio de 2015]. La Directiva entró en vigor en 1998.

[461] El Reglamento entró en vigor el 25 de mayo de 2016 pero se comenzó a aplicar dos años después, desde el 25 de mayo de 2018. Hasta entonces, tanto la Directiva 95/46/CE como las normas nacionales que la trasponen, seguían plenamente válidas y aplicables.

de protección de datos»[462]. Del mismo modo la Directiva se denomina "Directiva madre", precisamente porque es el texto de referencia a nivel europeo en el ámbito de la protección de datos personales[463].

97. La Directiva, adoptada sobre la base del antiguo artículo 95 TCE relativo a la aproximación de las legislaciones en el marco del mercado interior (actualmente artículo 114 TFUE), persiguió el objetivo de proteger los derechos y las libertades fundamentales de las personas, y en particular el derecho a la vida privada con respecto al tratamiento de las informaciones sobre la persona[464]. Por tanto, con ello se crea un marco armónico para la protección de la información personal, incluidos los datos personales no automatizados, para evitar un descarte excesivo en «*los niveles de protección de los derechos y libertades*» fundamentales, que puede obstaculizar no sólo la protección de las posiciones subjetivas sino también «*el ejercicio de una serie de actividades económicas a escala comunitaria*»[465]. Sin embargo, las disposiciones contenidas en la Directiva 95/46/CE[466] obligaban a los

[462] *Vid*. María Mercedes SERRANO PÉREZ (2003), *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, pág. 95; AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 18); Kristiina MILT (2019).

[463] Algunos autores la han descrito como Directiva "*omnibus*". En este sentido, *vid*. Patrick J. MURRAY (1997), «The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?», en *Fordham International Law Journal*, vol. 21, issue 3, pág. 941. Disponible en Internet: http://ir.lawnet.fordham.edu/ilj/vol21/iss3/10/ [consulta: 10 de agosto de 2017]; Joseph A. CANNATACI and Jeanne Pia MIFSUD-BONNICI (2005), «Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty», en *Information & Communications Technology Law*, vol. 14, issue 1, pág. 7.

[464] La Directiva 95/46/CE fue adoptada en una época en la que la "*World Wide Web*" comenzó a cobrar impulso, pero los términos tales como la Web y "*social web*" todavía no existían, del mismo modo que no existía una regulación internacional de la Red, cuya evolución, en paralelo a la invención constante de nuevas tecnologías y aplicaciones, ha hecho todavía más arduo la ambiciosa tarea. Esto planteó la cuestión de si la Directiva era aplicable a estos nuevos conceptos, que dependen en gran medida de la participación de los usuarios y la contribución de este último con su información personal. Neil ROBINSON, Hans GRAUX, Maarten BOTTERMAN (2008), *Review of EU Data Protection Directive: Inception Report*, Santa Monica, RAND Corporation, págs. 37. Disponible en Internet: http://www.rand.org/pubs/working_papers/WR607.html [consulta: 06 de agosto de 2017].

[465] Considerando 7 de la DIRECTIVA 95/46/CE.

[466] Imposible citar toda la inmensa bibliografía sobre la Directiva. A continuación, se ilustran algunas obras consultadas: Manuel HEREDERO HIGUERAS (1997), *La directiva comunitaria de protección de los datos de carácter personal: comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Pamplona, Aranzadi, págs. 375; Jesús María PRIETO GUTIERREZ (1997), «La Directiva 95/46/CE como criterio unificador», en *Revista del poder judicial*, núm. 48, págs. 165-234; Miguel Ángel DAVARA RODRÍGUEZ (1998), *La protección de datos en Europa: principios, derechos y procedimientos*, Madrid, Grupo Asnef-Equifax, págs. 204; Alvaro A. SÁNCHEZ BRAVO (1998); Mónica ARENAS RAMIRO (2006); María del Carmen GUERRERO PICÓ (2006: 585); Christopher KUNER (2007), *European Data Protection Law. Corporate Compliance and Regulation*, Second Edition, Oxford, Oxford University Press, págs. 592. ISBN: 9780199283859; Lucrecio REBOLLO DELGADO y María Mercedes SERRANO PÉREZ (2010), *Introducción a la protección de datos*, Madrid, Dykinson, págs. 258; Valentina COLCELLI (2014), «La protezione dei dati personali. Profili ricostruttivi tra mercato interno e ordinamento nazionale», en *Diritto e Processo*, págs. 411-468. ISSN: 1722-1110. Disponible en Internet: http://docplayer.it/3217576-Valentina-colcelli-1.html [consulta: 11 de noviembre de 2015]; Francesco MODAFFERI (2015), *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Roma, Lulu.com, págs. 374. ISBN: 9781326464059; Franco PIZZETTI (2016a), *Privacy e il diritto*

Estados a cumplir con ellas. El instrumento se adoptó en un momento en que varios Estados miembros ya habían adoptado leyes nacionales, dejando, no obstante, a las legislaciones nacionales la adaptación, en particular en lo que respecta a las normas sobre excepciones en áreas específicas[467]. En efecto, la Directiva 95/46/CE dejaba «*puerta la abierta*» al legislador nacional para adaptar la normativa a un régimen más amplio de excepciones[468], aunque, con muchas limitaciones, tuvo el mérito de "haber tratado de homogeneizar la legislación de «*los diferentes Estados miembros*» de la Unión".

98. Como se ha adelantado al empezar esta parte, el propósito de la libre circulación de mercancías, capitales, servicios y personas en el mercado interior ha requerido la libre circulación de los datos, que no podría lograrse si en los Estados miembros no hubiera un nivel elevado y uniforme de protección de datos. En los considerandos introductorios de la Directiva[469], se nota que entre los objetivos de la Comunidad hay que «*promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales*». También se subraya, que «*el establecimiento y funcionamiento del mercado interior,* (…) *hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas*». Además, en el considerando 7, se acentúa el aumento del intercambio de datos personales entre todos los sujetos de la vida privada en la vida económica y social (empresas y administraciones) y se menciona el riesgo de que la diferencia en los niveles de protección de las personas puede obstaculizar este intercambio contra el buen «*funcionamiento del mercado interior*»; de ahí la necesidad de una norma de

europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Torino, G. Giappichelli Editore, págs. 328.

[467] Shara MONTELEONE (2007), «La disciplina del trattamento dei dati personali in Europa», en *Teutas Law & Technology*. La Directiva fue aprobada por el Parlamento Europeo en una Resolución para regular el tratamiento de los datos personales, pero varios años después para que los Estados miembros acogieran y dieran cumplimiento a la Directiva en sus legislaciones nacionales. España ha implementado formalmente la Directiva 95/46/CE en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que modificó la LORTAD de 1992. La aplicación de la ley compete a la Agencia Española de Protección Datos (AEPD). En Italia, la ley sobre la protección de datos de carácter personal hace su primera aparición el 8 de mayo de 1997, con la entrada en vigor de la Ley de 31 de diciembre de 1996, n. 675, hecha bajo disposiciones comunitarias. Más tarde fue necesario reordenar la materia y se publicó el "*Codice in materia di protezione dei dati personali*", adoptado por Decreto Legislativo de 30 de junio 2003, n. 196. Alemania, por ejemplo, no se ha puesto en marcha antes de 2001, lo que demuestra claramente la complejidad de la ley que regula el tratamiento de datos personales. Elisenda BRU CUADRADA (2007), «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad», en *III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas*, organizado por los Estudios de Derecho y Ciencias Políticas de la UOC, núm. 5, págs. 78-92. Disponible en Internet: http://www.uoc.edu/idp/5/dt/esp/bru.pdf [consulta: 21 de diciembre de 2015].

[468] María del Carmen GUERRERO PICÓ (2005).

[469] Considerando 1 y 3 de la DIRECTIVA 95/46/CE.

ámbito comunitario de protección que sea «*equivalente en todos los Estados miembros*»[470]. El buen funcionamiento de las exigencias del mercado único exige que sean salvaguardados los derechos fundamentales de la persona.

99. Es decir, el texto tiene como objetivo concretizar los principios del derecho a la vida privada, ya contemplado en artículo 8 del CEDH[471], y del Convenio n. 108, de los cuales la Directiva es una aclaración y ampliación, al proteger los derechos y libertades de las personas. Al mismo tiempo, prohíbe a los Estados impedir la libre circulación de datos personales por motivos relacionados con la protección de la privacidad[472]. Hay que recordar que cuando se redactó la Directiva 95/46/CE, no había la CDFUE y, pues, el derecho a la protección de datos personales aún no había sido contemplado como un derecho fundamental autónomo en el Derecho originario o en el Derecho derivado de la UE[473]. En este sentido, la Directiva ha sido el primer acto normativo comunitario que trata específicamente la protección de los derechos y las libertades fundamentales[474].

100. La Directiva se refería a la protección de los derechos a la libertad personal, con respeto al tratamiento de datos personales y su movimiento dentro y fuera de la *ex* Comunidad Europea, dando cuenta al desarrollo que la sociedad tecnológica puede representar: tanto un estímulo para el progreso como un peligro potencial para el libre desarrollo de la persona. En ese sentido, la redacción del considerando 2, afirmaba que «*los sistemas de tratamiento de datos están al servicio del hombre; que deben,* (…) *respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad*», pero al mismo tiempo «*contribuir al progreso económico y social, al desarrollo de los intercambios* (…)».

---

[470] Considerando 8 de la DIRECTIVA 95/46/CE.
[471] Considerando 10 de la DIRECTIVA 95/46/CE. En el primer considerando de la Directiva se hace referencia al CEDH que, sin embargo, éste no menciona de forma expresa el concepto de derecho de protección de datos personales sino el de vida privada. El término oficial es "*privacy*" en términos del idioma en que fue redactada.
[472] *Vid*. considerando 11 de la DIRECTIVA 95/46/CE: «*Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales*».
[473] *Vid*. Lucrecio REBOLLO DELGADO (2004), *Derechos fundamentales y protección de datos*, Madrid, Dykinson, pág. 132; Elisenda BRU CUADRADA (2007: 81); Ricard MARTÍNEZ MARTÍNEZ (2007), «El derecho fundamental a la protección de datos: perspectivas», en *III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas*, organizado por los Estudios de Derecho y Ciencias Políticas de la UOC, núm. 5, págs. 47-61. Disponible en Internet: http://www.uoc.edu/idp/5/dt/esp/martinez.html [consulta: 23 de diciembre de 2015]; Alejandro Luis GACITÚA ESPÓSITO (2014: 176).
[474] Paolo PALLARO (2002: 81); Alessandra DI MARTINO (2005), «La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela», in Sergio P. PANUNZIO (a cura di), *I diritti fondamentali e le corti in Europa*, Napoli, Jovene, pág. 368.

101. La norma europea también testimonia la exigencia, en materia de derechos fundamentales, de crear un derecho constitucional común[475], basado en el intercambio de modelos culturales y legales. Esta tendencia favorece, por un lado, un proceso de homogeneización de los niveles de protección de los derechos, independientemente del sistema jurídico de referencia, y por otra parte, enriquece el contenido de los derechos reconocidos por las constituciones nacionales. De ahí el doble sentido de la Directiva, que requiere a legislaciones nacionales para actuar en la materia y, al mismo tiempo, introduce los principios que constituyen criterios para la interpretación de disposiciones constitucionales para proteger la confidencialidad.

102. La Directiva 95/46/CE nació con dos "contradictorios" objetivos: primero, evitar intromisiones ilegítimas en la vida de las personas por parte de los Estados miembros, garantizando "la protección de las libertades" y de "los derechos fundamentales de las personas físicas", en particular, "del derecho a la privacidad y el tratamiento de los datos personales": «*Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales*» (artículo 1, apartado 1); y segundo, asegurar la consecución del mercado interior y la «*libre circulación de datos*» sin restricciones injustificadas entre los Estados miembros[476]. En lugar de presentar la "privacidad" y la "libre circulación de datos" como conflictivos, la Directiva logra un equilibrio armonioso entre estos dos objetivos[477], que son reconocidos con una referencia a su igual dignidad.

---

[475] El ámbito territorial de la Directiva de protección de datos es de aplicación además de a los 28 Estados miembros de la Unión Europea, a los Estados no miembros de la UE que forman parte del Espacio Económico Europeo (EEE), tales como Islandia, Liechtenstein y Noruega. Con la Directiva de 1995, el legislador europeo ha entendido, por lo tanto, fijar un conjunto de normas y criterios con el fin de garantizar una protección uniforme de los datos personales en la UE. Sobre la creación de un derecho constitucional común en Europa, *vid*. María del Carmen GUERRERO PICÓ (2005).

[476] Artículo 1 (Objeto de la Directiva), apartado 2, de la DIRECTIVA 95/46/CE: «*2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1*». Desde el ámbito comunitario siempre se ha mostrado especial sensibilidad por conciliar la protección de datos con la libre circulación de datos personales, y así, esta preocupación se ha manifestado en la Directiva 95/46/CE que en su artículo 1, apartado 2. Por ello, la Directiva no se presenta como un texto restrictivo para la circulación de los datos personales en el ámbito comunitario, sino másbien al contrario, como el propio título de la Directiva revela, el verdadero espíritu que animó la elaboración del texto comunitario no fue otro que servir de instrumento para el libre flujo de datos personales en la Unión Europea. Ana Isabel HERRÁN ORTIZ (2003), *El derecho a la protección de datos personales en la sociedad de la información*, Bilbao, Universidad de Deusto, Instituto de Derechos Humanos, Cuadernos Deusto de Derechos Humanos, núm. 26, págs. 22-24. Disponible en Internet: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf [consulta: 25 de agosto de 2015]; María Mercedes SERRANO PÉREZ (2003: 95).

[477] Atando juntos dos intereses en conflicto, logró evitar el conflicto muy real entre los dos objetivos, pero fue expuesto a demasiadas críticas. Michael BIRNHACK (2008: 8).

103. A diferencia de otras normas anteriores, la fuente comunitaria en cuestión se aplicaba «*al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*» (artículo 3, apartado 1 - Ámbito de aplicación). Prevé que las disposiciones contenidas en la norma comunitaria cubren el tratamiento de datos personales, total o parcialmente automatizado, y no automatizado de datos personales contenidos o destinados a ser incluidos en los archivos[478]. Por lo tanto, el alcance material de la norma era bastante amplio, ya que contemplaba indeterminados tipos de información personal y en formatos indefinidos[479].

104. Al contrario, estaban excluidos del campo los tratamientos realizados por una persona física en el ejercicio de un uso «*exclusivamente personales o domésticas*» o materias reservadas a la soberanía de cada País en las que no se aplica el derecho comunitario, como la seguridad pública, la defensa o la seguridad del Estado[480]. En este sentido, el Convenio n. 108 tiene un importante punto de fuerza, ya que fue diseñado para que operase incluso en los sectores sensibles de la cooperación judicial en materia penal y de policía. Consecuentemente, las normas de la Directiva 95/46/CE «*no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal*» (artículo 3, apartado 2, primer guion). Los Estados estaban llamados a proveer con adecuadas normativas en los sectores excluidos por la aplicación. Según el artículo 3, apartado 2 de la Directiva, las leyes europeas

[478] El Convenio n. 108 se aplica, sin embargo, sólo a la información automatizada.

[479] Sin embargo, «*los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario*» (considerando 16). *Vid*. Alejandro Luis GACITÚA ESPÓSITO (2014: 178).

[480] *Cfr*. considerando 13: «*Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado*». También véanse los considerandos 16 y 43.

de protección de datos no son de aplicación en aquellos casos en los que el tratamiento de datos tenga un fin de «*seguridad pública, defensa, seguridad del Estado y actividades del Estado en el ámbito penal*»[481].

105. Por consiguiente, los ciudadanos europeos no estuvieron protegidos por las garantías contempladas bajo el tercer pilar, que no estaba cubierto por el Derecho comunitario en el sentido propio, siendo devuelto ampliamente a las determinaciones de los Estados. La jurisprudencia del Tribunal de Justicia ha dado una interpretación restrictiva de las categorías de excepciones. El Tribunal sostuvo que la excepción contenida contendría una lista no exhaustiva, pero -al mismo tiempo- se aplicaría sólo a aquellas actividades que se mencionan expresamente o que pueden incluirse en la misma categoría (*eiusdem generis*)[482]. A pesar de la aparente contradicción de esta hipótesis, parece coherente con la imposibilidad de limitar el alcance de las normas europeas, limitándolas a los tratamientos de datos relacionados con los artículos sometidos a la aplicación de la legislación de la UE[483]. En esta categoría de excepciones al ámbito de aplicación, a continuación, la jurisprudencia se refiere sólo a las actividades del Estado o de las autoridades estatales[484], distintos a la esfera de actividades de las personas (empresas y entidades privadas, incluidas las entidades religiosas, organizaciones de voluntarios y editores de periódicos).

106. El artículo 3 de la Directiva se convirtió en un obstáculo cada vez que la UE ha intentado incorporar un nuevo instrumento de intercambio de datos en el campo de la seguridad pública. Esta deficiencia significativa fue después subsanada. A resultas, varios sistemas de gestión de bases de datos que inicialmente se han creado en subsectores específicos: el Sistema de Información de Schengen (SIS); el Sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín; el Sistema de Información de Visados (VIS) y el Convenio Europol. Sin embargo, las soluciones fueron insatisfactorias debido a las normas sectoriales que habían transformado en un marco fragmentado y desigual (sobre este asunto, *vid*. *infra* Capítulo III).

[481] En el mismo sentido, Ana Isabel HERRÁN ORTIZ (2002: 130).
[482] TJUE, *Göta hovrätt (Suecia) contra Bodil Lindqvist*, asunto C-101/01, sentencia de 6 de noviembre de 2003, apartado 44.
[483] *Vid*. el apartado anterior sobre el artículo 16 del TFUE.
[484] TJUE, *Göta hovrätt (Suecia) contra Bodil Lindqvist*, apartado 43.

107. En 2008 el paradigma cambió con la adopción de la Decisión Marco del Consejo[485] sobre la protección de datos en asuntos policiales y judiciales, parte del antiguo tercer pilar. Hasta entonces se había preferido incluir en los instrumentos individuales de cooperación disposiciones de protección de datos, dando lugar sin embargo de esta manera a un caos de normas aplicables, con la consecuencia de producir inseguridad jurídica, confusión y posible discriminación. Tal especificidad del ámbito de aplicación incluye también los poderes asignados a las autoridades de control comunes establecidos para Schengen y Europol[486], así como Eurojust.

108. La Directiva reconocía unas categorías especiales de informaciones, relativas a los derechos fundamentales de la persona, indicados por el artículo 8, definidos «*datos sensibles*», donde el tratamiento puede entrar en conflicto con otros valores protegidos por el CEDH y las constituciones nacionales. Estos siguen el modelo de disposiciones similares contenidas en el Convenio n. 108[487]. La prohibición se para, sin embargo, antes del consentimiento expreso de la persona interesada, salvo que la legislación del Estado miembro prevea que éste no sea suficiente para derogar la prohibición impuesta[488]. También se admiten exenciones adicionales que los Estados miembros pueden establecer, con las garantías adecuadas, por «*motivos de interés público importantes*». El amplio margen de apreciación concedido a los Estados, sin embargo, cambia en caso de tratamiento de los «*datos relativos a infracciones, condenas penales o medidas de seguridad*»[489].

109. La Directiva establecía que las informaciones deberían, con el tiempo, ser siempre tratadas de forma compatible con los fines por los que han sido recogidas inicialmente. En este sentido, debe ser compatible con los propósitos iniciales el sucesivo tratamiento con

[485] Antes de la Decisión Marco de 2008, la única solución era cubrir este tipo de medidas bajo el paraguas del antiguo primer pilar, tal y como ocurrió con el acuerdo internacional para la recogida de datos de pasajeros entre las Comunidades Europeas y Estados Unidos en 2004, o la Directiva de conservación de datos adoptada en 2006 (*vid*. *infra* Capítulo IV).

[486] La Decisión Marco 2008/977/JAI no se aplicaba a Europol, pero sí a la transferencia de datos por los Estados miembros hacia Europol. Conny RIJKEN (2010), «Re-Balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters», en *Common Market Law Review*, vol. 47, issue 5, págs. 1455–1492.

[487] Artículo 8 (Tratamiento de categorías especiales de datos), apartado 1, de la DIRECTIVA 95/46/CE.

[488] Otros y ulteriores pueden ser las excepciones al impedimento: el tratamiento podría, de hecho, ser necesario para cumplir con las obligaciones o derechos del tratamiento en materia de trabajo; o el tratamiento concierne datos y hechos públicos de modo manifiesto del mismo interesado; o se hace necesaria para salvaguardar el interés la vida de la persona interesada o de un tercero, cuando el propietario de los datos sea físicamente o jurídicamente incapaz de dar su consentimiento (artículo 8, apartado 2).

[489] Corresponde al legislador nacional hacer un equilibrio entre los distintos derechos, pero la búsqueda de este equilibrio está sujeta a verificación por parte del juez constitucional y los órganos de la justicia comunitaria (artículo 8, apartado 5).

fines históricos, estadísticos o científicos, siempre que se le dé suficiente garantía por los Estados. De los datos, a continuación, siempre debe garantizarse la exactitud y actualización. En relación con la calidad de los datos, implica que las finalidades para las que procede sean lícitas y que el responsable tome todas «*las medidas razonables*» para «*garantizar*» que los datos sean exactos, pertinentes y actualizados (artículo 6). Es decir, el deber de adoptar medidas, de acuerdo con el caso, sin esperar solicitud del interesado. Esto también es compatible con el requisito de la "lealtad" o corrección, como una herramienta indispensable para dar a conocer el peligro en el uso de la información de los demás, elevando el nivel de diligencia por parte de los responsables[490].

110. Los principios establecidos en el artículo 6 de la Directiva también se contemplan en el artículo 5 del Convenio n. 108 (*cfr*. *supra*). Los dos "integran la esencia de la legislación europea en materia de protección de datos, como punto de partida para una regulación más detallada en los artículos posteriores de dicho instrumento". Toda la legislación posterior en materia de protección de datos, tanto a escala de la UE como del Consejo de Europa, deberá respetar estos principios, los cuales deberán lógicamente tenerse en cuenta a la hora de interpretar dicha legislación[491]. En aplicación también de la protección del principio de confidencialidad y transparencia, que inspira gran parte de la acción comunitaria, en todo caso, la conservación de las informaciones nunca debe exceder el tiempo necesario para lograr el propósito deseado. Pero este principio se ha visto perjudicado por la progresiva *desviación de uso* en los sistemas de información europeos, que se puede definir como la ampliación gradual en el uso de un sistema o base de datos más allá de su finalidad original[492]. Este hecho se ha producido en todos los sistemas de intercambio de datos en la UE para fines policiales (que se van a examinar en esta investigación: Europol, SIS, VIS y Eurodac), que se crearon inicialmente para controlar las fronteras europeas o para fines comerciales, pero se han tratado posteriormente como una herramienta de detección e investigación del delito. No obstante, los datos recogidos por estos sistemas son ahora

[490] Según el Grupo de Trabajo del Artículo 29, el principio de limitación de finalidad consiste en recoger datos personales para finalidades específicas, explícitas y legitimadas, que no pueden ser tratados de manera incompatible con la finalidad original. ARTICLE 29 DATA PROTECTION WORKING PARTY (2013c), Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, adopted on 2 April 2013, págs. 70. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [consulta: 05 de septiembre de 2015].

[491] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014: 68).

[492] EUROPEAN DATA PROTECTION SUPERVISOR (2012), Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) (Recast version), Brussels, 5 September 2012, págs. 22. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-05_EURODAC_EN.pdf [consulta: 07 de septiembre de 2015].

también accesibles por las agencias policiales de los Estados miembros y Europol para combatir el terrorismo y otros delitos graves.

111. Las garantías aseguradas a los datos pueden ser, sin embargo, limitadas para responder a la protección de los intereses públicos y privados. La excepción coincide, para los primeros, con el interés «*del Estado, la defensa, la seguridad pública*», con fines de prevención, así como para perseguir infracciones criminales o éticas, relevantes intereses económicos o financieros del Estado miembro, para llevar a cabo tareas de control en relación con el ejercicio de su potestad pública y para fines de investigación científica. Por lo tanto, además de las áreas en las que la Directiva no se aplicaba (*vid*. *supra* artículo 3), el artículo 13 (Excepciones y limitaciones)[493], apartado 1, dispone que «*los Estados miembros podrán adoptar medidas legales para limitar*» el derecho de acceso e información" a los involucrados en el trato, cuando tales restricciones constituyen una medida necesaria (principio de necesidad) para la salvaguardia de las siguientes cuestiones: «*la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas*»[494].

112. En concreto, la Directiva establecía que cada Estado miembro, en los casos en que lleve a cabo uno de los objetivos mencionados anteriormente, pueda decidir limitar los principios - derecho de acceso e información - contenidos en los artículos siguientes: artículo 6, apartado 1[495]; artículo 10 (Información en caso de obtención de datos recabados del propio

[493] Para una visión general de las excepciones y limitaciones, véase *supra* también la Declaración n. 20 relativa al artículo 16 del TFUE.

[494] Al examinar los límites de la desviación de uso de los datos personales, según el Grupo de Trabajo del Artículo 29, debe tenerse en cuenta el principio de necesidad. El Grupo ha remarcado que es posible restringir el principio de limitación de finalidad si ello es estrictamente necesario para salvaguardar ciertos intereses de gran importancia. ARTICLE 29 DATA PROTECTION WORKING PARTY (2013c). Sin embargo, el problema es que no existen parámetros estrictos para evaluar la necesidad de que las agencias policiales accedan a los datos almacenados en sistemas de información de la UE.

[495] Artículo 6, apartado 1, de la DIRECTIVA 95/46/CE: «*Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con*

interesado); artículo 11 (Información cuando los datos no han sido recabados del propio interesado), apartado 1; y en los artículos 12 (Derecho de acceso) y 21 (Publicidad de los tratamientos). "Estas excepciones y limitaciones deben interpretarse de acuerdo con lo dispuesto en el artículo 8 del CEDH"[496].

113. La búsqueda de un equilibrio entre el derecho a la protección de los datos personales y otros derechos e intereses en conflicto pasa inevitablemente por el principio de necesidad, por lo que, en su aplicación, ello parece ser sustancialmente equivalente al de proporcionalidad: el derecho de la persona a la que los datos se refieren puede ser sumiso en favor de otro derecho fundamental o de un interés digno de protección, pero sólo en la medida en que ello sea necesario. Además, entre las diversas alternativas disponibles, debería preferirse aquel que, permitiendo alcanzar el objetivo establecido, produzca la menor restricción necesaria del derecho en cuestión.

114. Es especialmente destacable, en este sentido, la introducción, por primera vez, en cada Estado, de instituir una autoridad de control independiente[497], con funciones de vigilar, en el territorio, para la aplicación de la Directiva, reconocimiento que se hizo en el Consejo de Europa sólo más tarde, en el Protocolo Adicional al Convenio n. 108[498]. Las autoridades nacionales de control (también llamadas autoridades garantes) deben ser siempre

relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos».

[496] *Vid*. considerando 10 de la DIRECTIVA 95/46/CE: «*Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contratrio, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad*».

[497] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2010), *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 8 y ss. Disponible en Internet: http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities [consulta: 21 de noviembre de 2015]. A diferencia del modelo americano, el modelo europeo de privacidad puede contar con la presencia de autoridades de control independientes específicas que representan una garantía para el cumplimiento de las normas relativas a la privacidad. La no inclusión de autoridades independientes específicas en el modelo estadounidense podría encontrar una justificación en la ideología de "*laissez-faire*" y "*laissez-passer*" que llevó al legislador estadounidense a reponer una extraordinaria confianza en la autoreglamentación. Sobre este tema, *vid*. Ugo PAGALLO (2008), *La tutela della privacy negli Stati Uniti d'America ed in Europa. Modelli giuridici a confronto,* Milano, págs. 96 y ss.

[498] *Vid*. *supra*, PROTOCOLO ADICIONAL AL CONVENIO n. 108, artículo 1 (Autoridades de control).

consultadas por los Estados miembros en la elaboración de medidas reglamentarias o administrativas relativas al tratamiento de los datos. Las autoridades de control tienen poderes investigadores y de intervención y son las receptoras de preguntas sobre control presentadas por parte de personas o asociaciones que las representan, cuando crean violados estos derechos.

115. La decisión de confiar la función reguladora a una autoridad de control independiente también en el RGPD[499] parece sin duda apropiada: el equilibrio entre los derechos e intereses en conflicto, de hecho, puede ser implementado de manera efectiva por un ente/persona que tenga conocimientos técnicos cualificados, a menudo indispensables para la mejor solución de los conflictos en la materia. En este sentido, se hace constar que los tribunales nacionales, al tiempo que proporcionan garantías de experiencia legal, a menudo no tienen el suficiente grado de preparación técnica. Tendrían que ser acompañados por profesionales con conocimientos técnicos; sin embargo, el instrumento jurídico de experiencia o asesoramiento técnico sería inadecuado para la función reguladora, ya que se pretende resolver una disputa específica, así como insuficiente para garantizar la imparcialidad de la decisión, más fácilmente sometida a las influencias externas. Por otra parte, sería inútil proclamar los derechos de acceso, rectificación o cancelación en relación con los datos personales, con la obligación de tratarlos de manera leal y lícita, con el consentimiento informado de los interesados y con las medidas de seguridad previstas por ley si, en la práctica, no fuera previsto el control preciso de una autoridad[500].

116. En relación con las funciones[501], la Directiva de protección de datos establecía en el apartado 6 del artículo 28 que toda autoridad de control será competente para «*ejercer en el territorio de su propio Estado miembro los poderes*» reconocidos en el artículo 28. Es

[499] *Vid*. Capítulo VI, Autoridades de control independientes, del RGPD.
[500] Ugo PAGALLO (2008: 132).
[501] La Directiva prevé que sus competencias serán las siguientes: vigilancia de «*la aplicación en su territorio de las disposiciones adoptadas por ellos*» en aplicación de la Directiva 95/46/CE; obligación de consulta por parte de los Estados nacionales «*en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal*»; poder de investigación «*como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control*»; poderes de intervención, tales como «*formular dictámenes antes de realizar los tratamientos,* (…) *y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales*»; capacidad procesal «*en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial*». Artículo 28 (Autoridad de control) de la DIRECTIVA 95/46/CE.

importante destacar este punto que ha sido analizado e interpretado en la sentencia del TJUE de 6 de octubre de 2015, caso *Schrems contra Facebook* (*vid*. Capítulo IV *infra*).

117. Las autoridades, sin embargo, no son los únicos organismos creados para perseguir los objetivos de la Directiva. Esta última, de hecho, proporcionaba además del control independiente de la autoridad nacional (que tiene competencia nacional), un grupo de trabajo de alto nivel sobre "protección de las personas en lo que respecta al tratamiento de datos personales" (Capítulo VI de la Directiva). En este sentido, el artículo 29 de la Directiva 95/46/CE constituye a nivel europeo un "Grupo de protección" de las personas con respecto al tratamiento de los datos (llamado Grupo de Trabajo del Artículo 29 o en inglés *Article 29 Working Party*)[502]. Compuesto por representantes de las autoridades de los Estados miembros de la Unión Europea y por un representante de la Comisión, es un órgano de especial importancia en esta materia, que tiene carácter consultivo e independiente[503]. Aunque las funciones del Grupo principalmente consisten en la formulación de recomendaciones, emisión de asesoramiento técnico y la elaboración de normas comunes**,** es una actividad esencialmente consultiva. A la interpretación de la misma se debe dar una innegable importancia a la luz de la permanente cooperación que permite a las autoridades nacionales incidir sobre el proceso decisional europeo y facilitar la aplicación uniforme de la legislación europea.

118. Desde la entrada en vigor de la Directiva 95/46/CE, el Grupo, de hecho, se ocupó del área de las relaciones exteriores de la Unión, con especial referencia a la «*transferencia de datos personales a terceros países*». Como se ha explicado, la regla en este sentido es el *ex* artículo 25 de la Directiva, que admitía la posibilidad de la transferencia de datos personales hacia países terceros sólo si ese asegura un «*nivel de protección adecuado*»[504]. Las actividades del Grupo no sólo se limitan a este aspecto. En esta línea, se ha relacionado con los diversos temas relacionados con la privacidad y la protección de los datos personales, entre ellos la lucha contra el terrorismo[505]. El Grupo tiene función de proporcionar

[502] Sitio web del Grupo de Trabajo del Artículo 29: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
[503] Artículo 29 (Grupo de protección de las personas en lo que respecta al tratamiento de datos personales) de la DIRECTIVA 95/46/CE.
[504] ARTICLE 29 DATA PROTECTION WORKING PARTY (2000), Working Document. Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on 21st November 2000, 5063/00/EN/FINAL, WP 37, págs. 99. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf [consulta: 14 de enero de 2016].
[505] ARTICLE 29 DATA PROTECTION WORKING PARTY (2001), Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, adopted on 14 December 2001, 0901/02/EN/Final, WP 53,

dictámenes, tanto en el ámbito de la protección de datos en Europa como en la aplicación más homogénea de la legislación comunitaria en los Estados miembros[506].

119. Evolución en parte similar se ha producido con la creación de la figura de Supervisor Europeo de Protección de Datos, sobre la base del artículo 286 del TCE introducido por el Tratado de Ámsterdam[507]. Ahora bien, a este "órgano supervisor independiente", responsable de controlar «*la aplicación de actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos*»[508] a las instituciones, organismos y agencias, no se le atribuyeron competencias sobre las áreas de la cooperación judicial en materia penal y en el de la cooperación policial[509], pero la necesidad de un instrumento a este respecto se reconoce en el considerando 17 del Reglamento instituyente[510]. Este necesario avance sólo se logró hacer realidad en 2008, con

---

págs. 4. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp53_en.pdf [consulta: 08 de enero de 2016]. La Directiva de 1995 contenía un capítulo (Capítulo IV) dedicado a las normas sobre la transferencia de datos personales a países terceros. Entre los objetivos declarados sea de la Directiva sea de la nueva legislación (Reglamento) es la circulación de datos el que es indispensable para la realización del mercado único europeo. La transferencia de datos, en diferentes formas de transmisión, comunicación y difusión, se dedica, de hecho, en gran parte a la legislación sobre protección de datos. Precauciones ordinarias tienden a tensarse si esas transferencias que afecten a terceros países no proporcionan el mismo nivel de protección de los datos personales reconocidas en Europa. Será, por lo tanto, la Comisión quien tiene la obligación de hacer una "evaluación de la adecuación" de los terceros países, a la luz de los índices predefinidos, tanto en virtud de la Directiva que del Reglamento. El espíritu, de hecho, es prohibir la transferencia de datos personales cuando el Estado destinatario del flujo de datos no ofreczca un nivel adecuado de protección y, a la inversa, permitirlo, sólo cuando el Estado tercero de destino asegure, sin embargo, dicho nivel de protección. En otras palabras, tiene como objetivo garantizar que los datos personales de sus ciudadanos siguan disfrutando de un alto nivel de protección incluso si dejan el territorio de los Estados miembros. Sobre la transferencia de datos personales a terceros países u organizaciones internacionales, véase la nueva normativa del RGPD en el Capítulo V.

[506] Este último es responsable de: «*a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros; c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades; d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria*». Artículo 30, apartado 1, de la DIRECTIVA 95/46/CE.

[507] La primera aproximación que cabe hacer es que se trata de un órgano de "reciente creación", concretamente del año 2001 y de conformidad con el artículo 286 del TCE, antiguo 213 B, añadido por el Tratado de Ámsterdam de 2 de octubre de 1997: «*a partir del 1 de Enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de los datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente tratado o sobre la base del mismo*».

[508] En Lucrecio REBOLLO DELGADO (2014: 157).

[509] El SEPD, desempeña un papel relevante, bajo el manto de la Unión Europea; esto es así cuando simplemente y a modo de ejemplo se contempla el gran número de dictámenes en los que participa, realizando grandes consideraciones sobre un asunto en concreto de la protección de datos. Sobre el SEPD, *vid*. *amplius* Javier ÁLVAREZ HERNANDO (2011), *Guía práctica sobre Protección de Datos: cuestiones y formularios*, Lex Nova, pág. 573; Lucrecio REBOLLO DELGADO (2014: 157 y ss.).

[510] Considerando 17 del REGLAMENTO (CE) N. 45/2001: «*La eficacia de la protección de las personas respecto al tratamiento de datos personales en la Unión requiere la coherencia de las normas y de los procedimientos aplicables en la materia a las actividades correspondientes a diferentes marcos jurídicos. La*

la adopción de la Decisión Marco 2008/977/JAI del Consejo, relativa a la protección de datos personales en las áreas citadas.

4.1.1. La insuficiencia de la Directiva para abordar los riesgos que plantea la privacidad en un mundo global

120. El análisis de las características más destacadas de la Directiva que interesan a esta investigación nos lleva a algunas reflexiones. Tras más de 20 años, el contexto en el que se estableció la Directiva ha cambiado profundamente y ya se han impugnado algunos supuestos básicos de la misma y ha sido sustituida por un marco jurídico nuevo, coherente y más armonioso, para salvaguardar el derecho fundamental a la protección de datos en la Unión Europea. Antes de seguir, esto conduce a la pregunta que nos hemos planteado con el presente apartado.

121. Por supuesto, la Directiva 95/46/CE disciplinó las actividades en el marco comunitario, en virtud de las competencias atribuidas a la Comunidad de los Estados. Sin embargo, el uso del instrumento comunitario de la Directiva se revela al final poco útil para asegurar la uniformidad legislativa solicitada dentro de los países miembros de la UE, siendo reconocido un amplio margen de discrecionalidad a cada Estado en cuanto a las modalidades y formas de aplicación[511], lo que no ha hecho posible la realización de un marco regulatorio

elaboración de principios fundamentales relativos a la protección de datos personales en el ámbito de la cooperación judicial en materia penal y en el de la cooperación policial y aduanera, y la creación de una secretaría para las autoridades de control comunes, establecidas en virtud del Convenio Europol, el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros y el Convenio de Schengen, constituyen a este respecto una primera etapa». Ahora Reglamento (UE) 2018/1725.

[511] El 15 de mayo de 2003 la Comisión transmitió al Parlamento el Primer Informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE) (COM (2003) 265), y luego una Propuesta de Resolución del Parlamento Europeo sobre el Primer Informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE) (COM (2003) 265 – C5-0375/2003 – 2003/2153(INI)). INFORME DE LA COMISIÓN - PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46 CE), COM/2003/0265 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52003DC0265 [consulta: 09 de febrero de 2016]; INFORME SOBRE EL PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46/CE), (COM (2003) 265 – 2003/2153(INI)), Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores, Final A5-0104/2004, 24 de febrero de 2004. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2004-0104+0+DOC+XML+V0//ES [consulta: 09 de febrero de 2016]. Los Informes muestran que las instituciones están de acuerdo en que se alcance el objetivo de nivelación y estandarizar las diferentes legislaciones nacionales en materia de protección de datos entre los Estados miembros. Estas disparidades impiden a las organizaciones multinacionales para definir políticas paneuropeas sobre protección de datos. Las principales dificultades que surgieron con respecto a la aplicación de la directiva europea sobre protección de datos son esencialmente tres: a) la falta de recursos de aplicación; b) el respeto de la norma por los responsables del tratamiento desigual; c) la falta de conocimiento de los derechos de las personas interesadas. Pero al mismo tiempo la Comisión Europea señaló que no había ninguna razón para llegar a una nueva Directiva y que era necesario aprovechar mejor el marco jurídico existente. La Comisión consideró que la Directiva "cumple sus objetivos originales" y, por lo tanto, no prevé presentar ninguna propuesta legislativa para modificarla. Sobre las críticas y la necesidad de revisión de la aplicación de la Directiva de 1995, muy importante es el estudio

armónico sobre la privacidad. Por ejemplo, la Directiva ha sido transpuesta de manera rigurosa por los ordenamientos jurídicos más garantistas, proporcionando sistemas de salvaguardias adicionales. Se considera especialmente la experiencia española, italiana, francesa y alemana. Por otra parte, los Países del norte de Europa de tradición anglosajona mantuvieron un perfil bajo, optando por una aplicación "*soft*" (suave) de las disposiciones establecidas en Europa[512]. La extrema fragmentación que se produjo daba lugar a muy diversos niveles de protección en cada País, con repercusiones negativas tanto para los ciudadanos como para las empresas.

122. Las incoherencias en la protección de datos en los Estados miembros de la UE también han sido señaladas a la Comisión Europea, la necesidad de una regulación única y armoniosa de la protección de datos que abarque todo el territorio de la UE, en particular para reducir el margen de discrecionalidad de los legisladores nacionales, de las autoridades de control y de los tribunales. Por lo tanto, la armonización de las normas aplicadas en los distintos Estados miembros se ha visto como una prioridad en el nombre de la fórmula «*Un continente, una ley*»[513]. También el Tribunal de Justicia, consciente del problema que plantea la fragmentación de las legislaciones de protección de datos en Europa y de las diferentes aplicaciones entre los Estados miembros, ha reiterado la importancia de los objetivos perseguidos por la Directiva 95/46/CE, manteniendo un equilibrio entre la libre circulación de los datos personales y la salvaguardia del derecho a la intimidad. En este sentido, es indudable que la Directiva 95/46/CE no garantizaba plenamente ninguno de sus principales objetivos.

123. Siguiendo con los límites de la norma europea, la Directiva excluía expresamente la aplicación al tratamiento de datos personales realizado en el ejercicio de actividades no comprendidos en el ámbito del derecho comunitario[514], así como el problema de la

del Profesor Korff. *Vid*. Douwe KORFF (2002), *EC Study on Implementation of Data Protection Directive 95/46/EC*, REPORT on the findings of the study by Douwe Korff consultant to the European Commission, págs. 253. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 [consulta: 11 de febrero de 2016].

[512] Douwe KORFF (2002).

[513] COMISIÓN EUROPEA - Comunicado de prensa (2015c), El acuerdo sobre la reforma de la protección de datos promovida por la Comisión reforzará el mercado único digital, Bruselas, 15 de diciembre de 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-6321_es.htm [consulta: 10 de febrero de 2016].

[514] *Vid*. VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA, Título V (Disposiciones generales relativas a la acción exterior de la unión y disposiciones específicas relativas a la política exterior y de seguridad común y Título VI (Disposiciones finales).

transferencia de datos personales a terceros países[515] y las amenazas planteadas por la injerencia del Estado y por parte de terceros a la protección de la privacidad. Eso, pone de relieve el déficit de aplicación de la Directiva a las operaciones de procesamiento relativa a la seguridad pública, la defensa y la seguridad del Estado, todavía reguladas de modo parcial y fragmentario respecto a las específicas disposiciones nacionales[516], que pudieran causar diferencias en la aplicación de las normas comunitarias, sobre todo después de los ataques terroristas que azotan el mundo occidental desde la década de 2000, y que llevaron a reconocer la necesidad de armonizar la legislación existente en un marco común, equilibrando la necesidad de confidencialidad del individuo con el interés superior de la seguridad interna de los Estados miembros.

124. Además, a lo largo del tiempo, debido a los desarrollos tecnológicos, se han cuestionado los supuestos básicos de la Directiva, lo que cuestiona tanto su capacidad de ajustarse a los objetivos para los que se adoptó en 1995 como de conservar su influencia hasta ahora global. La Directiva tampoco fue suficientemente actualizada para mantener el ritmo de la evolución de las nuevas tecnologías[517], lo que lleva a ambigüedades y a interpretaciones peligrosas, al menos por el riesgo de que se desvíen de la voluntad del legislador europeo. De hecho, aunque toma nota de la evolución positiva del derecho a la

[515] Más detalle sobre este tema, *vid*. la jurisprudencia del TJUE y las normas del nuevo Reglamento.

[516] En este mismo sentido, el Parlamento Europeo en su Resolución, critica los gravísimos retrasos acumulados por la Comisión e insta a la misma a proponer «*un "instrumento jurídico" para la protección de la vida privada; dicho instrumento tendrá carácter obligatorio y se destinará a garantizar en el tercer pilar el mismo grado de protección de los datos y de la vida privada* (…)», en el contexto de la cooperación policial y la asistencia jurídica mutua en materia penal, en particular con referencia a Europol y Eurojust, para llegar a la definición, lo antes posible, de un verdadero ELSJ que se caracterice por la cooperación contra la delincuencia a nivel supranacional. INFORME SOBRE EL PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46/CE). En la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, la Comisión, tomando nota de una mejoría en la aplicación de la Directiva, no considera necesario intervenir con las enmiendas, sobre todo porque las empresas, mediante la adaptación de su negocio a nuevos preceptos, ya han incurrido en costos. También se considera la Directiva 95/46/CE un marco jurídico general que cumpla con sus objetivos originales, como una garantía suficiente para el funcionamiento del mercado interior al tiempo que garantiza un alto nivel de protección. Representa un punto de referencia en muchos ámbitos de la acción, es neutral hacia la tecnología y sigue proporcionando respuestas sólidas y adecuadas a los problemas de este tipo. Según la Comisión, en cambio, hay dos aspectos de la norma que requerirá algunos cuidados: la independencia y autonomía de las autoridades supervisoras nacionales encargadas de la aplicación de la Directiva y el grado de autonomía de algunas disposiciones de la Directiva. Por último, la Comisión llama la atención sobre la necesidad de proporcionar, en el camino de la mejora legislativa sobre protección de datos a nivel europeo, procedimientos más eficientes en el ELSJ, de conformidad con los preceptos en los tratados actuales. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, COM/2007/0087 final, Bruselas, 7.3.2007. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007DC0087 [consulta: 16 de enero de 2016].

[517] *Vid*. Paul OHM (2010), «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», en *UCLA Law Review*, vol. 57, núm. 6, págs. 1701–1777. Disponible en Internet: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 [consulta: 02 de noviembre de 2015].

privacidad y la circulación de datos dentro de la Unión, se produjeron marcos regulatorios insuficientemente armonizados entre los Estados miembros. Este vacío fue cubierto, en parte, como explicará en detalle más adelante, por el Tribunal de Justicia de la UE (*vid*. Capítulo IV *infra*), que, en algunas de sus sentencias de referencia en este ámbito, ha logrado avances donde el legislador de la Unión ha fracasado. Hoy más que nunca, hay que darse cuenta de que la protección de datos personales es un derecho fundamental real que se refiere a las acciones cotidianas de todos nosotros y, al mismo tiempo, la libre circulación de datos personales es esencial para que los ciudadanos europeos puedan actuar y operar libremente dentro de un espacio común.

125. Con los límites que se les reconocen, la presente Directiva ha sido la piedra angular para la protección de la privacidad en la Unión Europea y, al mismo tiempo, ha logrado garantizar que esta protección no sea un límite para el libre flujo de información entre los Estados miembros[518], siendo este uno de los elementos fundamentales del mercado único.

126. A partir de 1995, la Directiva provocó una ola de reformas tanto en los Estados miembros de la UE como a nivel mundial. Debido a la Directiva, a nivel comunitario, las diferencias entre las normas jurídicas de los Estados miembros se han reducido, y a nivel mundial se atribuye a la Directiva una forma única de "*soft legal globalization*"[519] (globalización jurídica suave). Las leyes de protección de datos de otros países (como Australia, Israel, Japón, *etc*.) y de las regiones (América Latina y Asia) se inspiran en la Directiva de la UE, que se reconoce como el motor principal de un nuevo régimen jurídico mundial en materia de protección de datos. Además, la Directiva 95/46/CE cubre disposiciones determinadas para la transferencia de datos personales fuera de la Unión Europea, con el fin de asegurar la mejor protección posible.

127. De todos los instrumentos analizados anteriormente, la Directiva de la UE se ha convertido, en gran medida, en la guía de directrices y referencia para la protección de datos en todo el mundo. Sin embargo, para que la Directiva pueda ejercer sus principios a nivel mundial de manera más eficiente, debe revisarse y simplificarse para hacer frente a los nuevos desafíos. En este punto, la necesidad de uniformidad dentro de la Unión, así como la necesidad de adaptar la regulación que, a pesar de las intervenciones jurisprudenciales

[518] Richard MORGAN, Ruth BOARDMAN (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell, págs. 450.
[519] Michael D. BIRNHACK (2008: 1).

recientes, se remonta hace más de veinte años. Las discrepancias en la protección de datos en los Estados miembros de la UE también se destacaron ante la Comisión Europea, con la necesidad de una regulación única y armoniosa de la protección de datos que abarque todo el territorio de la UE, en particular para eliminar o reducir el margen de elección para los legisladores nacionales, las autoridades de control y los tribunales. Por lo tanto, la necesidad de garantizar el derecho fundamental a la protección de datos personales y una aplicación uniforme en todas las políticas de la UE ha llevado a la Comisión a proponer "un enfoque integral y coherente que garantice que el derecho fundamental a la protección de datos para las personas sea plenamente respetado"[520]. Después años de largas negociaciones, eso nos lleva a la aprobación del Reglamento de la UE n. 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que se deroga la Directiva 95/46/CE, innovando de manera significativa la disciplina (*infra*, Capítulo V).

4.2. La Decisión Marco 2008/977/JAI: ¿un documento de "cooperación policial" o un texto de "protección de datos"?

128. En la protección de la privacidad y protección de datos personales en el ELSJ de la Unión Europea, en más de una situación, ha resultado difícil de distinguir claramente los límites entre los diferentes pilares, en particular en el preexistente tercer pilar, relacionado con las cuestiones de la cooperación judicial en materia penal y policial. En esta materia, se han seguido aplicando las normas nacionales dictadas, teniendo principalmente en cuenta los principios del mencionado Convenio n. 108, así como un número de otras herramientas que también se han sumado a lo largo del tiempo en ausencia de un plan único a nivel comunitario, y que se han referido al Convenio de Estrasburgo como norma mínima[521]. En este contexto, tardíamente[522], se adoptó la Decisión Marco 2008/977/JAI del Consejo, de

[520] *Vid*. Efrén DÍAZ DÍAZ (2016), «The new European Union General Regulation on Data Protection and the legal consequences for institutions», en *Church, Communication and Culture*, 1:1, págs. 206-239. Disponible en Internet: https://doi.org/10.1080/23753234.2016.1240912 [consulta: 21 de abril de 2019].

[521] Paul DE HERT, Vagelis PAPAKONSTANTINOU and Cornelia RIEHLE (2008: 121 y 162). Se desprende de las normas que rigen el funcionamiento del Sistema de Información de Schengen (SIS y SIS II) y el Sistema de Información de Visados (VIS) o con el que se regulan el flujo de informaciones necesarias para la consecución de los fines institucionales de Europol (y Eurojust) o también en el Tratado Prüm. Para más detalles *vid*. *infra* Capítulo III.

[522] La propuesta de este instrumento se remonta al 2005, que había sido propuesta por la Comisión al mismo tiempo, se convertirá en la Decisión Marco 2006/960/JAI sobre la aplicación del principio de disponibilidad. Las dos propuestas son el fruto, de acuerdo con el Programa de La Haya, de la idea de desarrollar el alcance de la cooperación policial, lo que facilita el intercambio de información y, al mismo tiempo, la introducción de las normas europeas de protección de datos personales, el primer derecho fundamental que se pone en riesgo mediante el intercambio de información. El proceso de adopción de la Decisión Marco 2008/997/JAI ha durado mucho tiempo y se ha encontrado con dificultades debido en parte a las diferentes posiciones adoptadas internamente al Consejo, también a las fuertes fricciones entre el Consejo y el Parlamento Europeo en algunos puntos. Para un análisis detallado del recorrido que ha llevado a la adopción de la Decisión Marco véase Stefano CIAMPI (2009: 45-56; 64-75) y Paul DE HERT e Vagelis PAPAKONSTANTINOU (2009), «The data

hecho, para equilibrar la introducción a nivel comunitario del llamado principio de disponibilidad[523], que establece que las informaciones necesarias para contrastar la delincuencia (incluidas las personales) van, sin obstáculos, más allá de las fronteras interiores de la UE.

129. Como ha sido comentado anteriormente, la Directiva 95/46/CE se aplicaba solamente a las materias del primer pilar, permaneciendo ajena a los asuntos del segundo y tercer pilar (Política Exterior y de Seguridad Común; Cooperación policial y judicial en materia penal)[524]. Así pues, según el artículo 3, apartado 2, de la Directiva 95/46/CE, las leyes europeas de protección de datos no son de aplicación en aquellos casos en los que el tratamiento de datos tenga un fin de "seguridad pública, defensa, seguridad del Estado y actividades del Estado en el ámbito penal". Esta disposición se ha convertido en un obstáculo cada vez que la UE ha intentado incorporar un nuevo instrumento de intercambio de datos en el campo de la seguridad pública.

130. A pesar de que la legislación europea existente en el campo no sea particularmente sensible a estas necesidades, ya que no establece límites estrictos al intercambio de datos, según lo dispuesto en la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales en el marco de la cooperación policial y judicial en materia penal[525], se pretendía, artículo 1 (Objetivo y ámbito de aplicación), apartado 1, «(…) *garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular de su derecho a la intimidad en lo que*

protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for», en *Computer Law and Security Review*, núm. 25, pags. 403–414. Disponible en Internet: http://www.vub.ac.be/LSTS/pub/Dehert/270.pdf [consulta: 20 de enero de 2016].

[523] DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final), (2006/C 116/04), *Diario Oficial de la Unión Europea*, C 116, 17.5.2006, págs. 8–17. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52006XX0517(01) [consulta: 22 de enero de 2016]. *Vid*. puntos números 27 y 28.

[524] Ofelia TEJERINA RODRÍGUEZ (2014: 80 y ss.); María ÁLVAREZ CARO (2015), *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Madrid, Editorial Reus, págs. 65 y ss. De hecho, la Directiva 95/46/CE en el artículo 3, apartado 2, excluye de su ámbito de aplicación, el tratamiento de datos personales «(…) *efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal* (…)».

[525] DECISIÓN MARCO 2008/977/JAI DEL CONSEJO, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, *Diario Oficial de la Unión Europea*, L 350 de 30.12.2008, págs. 60–71. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008F0977 [consulta: 09 de julio de 2015].

respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública»[526]. El objetivo de la norma en estudio es por tanto «*la determinación de normas comunes para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal*» (considerando 42).

131. Antes de la adopción de la Decisión Marco[527], la colaboración entre las naciones en materia judicial ha sido caracterizada, en lo que respecta al intercambio de datos personales, por una serie de bases de datos de origen europeo, que de hecho representaron las únicas fuentes normativas para proteger el cambio de informaciones entre los Estados en ámbito judicial[528]. De esta prospectiva, la Decisión Marco fue el primer instrumento europeo adoptado para la protección de los datos en esta área[529] (tercer pilar). En este sentido, la Decisión está basada[530], en gran medida, en los principios y definiciones incluidos en el Convenio n. 108[531] y en la Directiva de protección de datos de 1995, y define un conjunto

[526] La Decisión Marco se basa en los antiguos artículos 30 del TUE, hoy en día los artículos 87-88 del TFUE.
[527] El proceso de adopción de la Decisión Marco 2008/997/JAI del Consejo, ha sido larga y se ha encontrado con dificultades debido, no sólo, a las diferentes posiciones adoptadas internamente al Consejo, sino también a la fuerte fricción entre el Consejo y el Parlamento sobre algunos puntos. *Vid*. Stefano CIAMPI (2009); Paul DE HERT e Vagelis PAPAKONSTANTINOU (2009); Alejandro Luis GACITÚA ESPÓSITO (2014: 195).
[528] En este sector nos referimos a instrumentos de cooperación intergubernamental. La protección de los datos utilizados para fines de seguridad, la policía y la justicia está regulada por normas sectoriales, en convenios o tratados particulares, que prevén la institución de varias autoridades de control común. Se hace referencia en particular al Convenio de Schengen, Europol, Eurodac y Vis. *Vid*. *infra* Capítulo III.
[529] *Vid*. EUROPEAN DATA PROTECTION SUPERVISOR - Press Release (2008), EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step, Brussels, Friday 28 November 2008. Disponible en Internet: https://edps.europa.eu/press-publications/press-news/press-releases/2008/edps-sees-adoption-data-protection-framework_en [consulta: 12 de julio de 2015].
[530] La Decisión trae causa, sobre todo, del «*Programa de La Haya sobre la consolidación de la libertad, la seguridad y la justicia en la Unión Europea, adoptado por el Consejo Europeo el 4 de noviembre de 2004, subrayaba la necesidad de un planteamiento innovador del intercambio transfronterizo de información policial, cumpliendo estrictamente condiciones fundamentales en el ámbito de la protección de datos*» (considerando 4). También *vid*. *supra*. Tal como afirman los considerandos de la Decisión, la norma tiene por objeto establecer los principios que han de regir la transferencia de datos entre Estados miembros, de conformidad con el principio de libre disponibilidad de la información establecido en el Programa de La Haya, en relación con las actuaciones practicadas en el marco del anterior tercer pilar. Ello porque la Directiva 95/46/CE se aplica exclusivamente al tratamiento de datos personales realizado en el ámbito del derecho comunitarizado, y «*no se aplica al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las contempladas en el título VI del Tratado de la Unión Europea, ni, en ningún caso, a las operaciones de tratamiento de datos relacionadas con la seguridad pública, la defensa, la seguridad del Estado o las actuaciones del Estado en materia penal*» (considerando 5). Este diferente ámbito de aplicación de ambas normas ha de entenderse subsistente después de la entrada en vigor del Tratado de Lisboa.
[531] Este parece ser el caso de las disposiciones sobre la utilización ulterior de datos transmitidos por otro Estado miembro (artículos 3 y 11) y el derecho de acceso a los datos (artículo 17). *Vid*. Zeno GERADTS, Peter SOMMER (2008) (eds.), *D6.7c: Forensic Profiling*, Future of Identity in the Information Society (FIDIS), pág. 59. Disponible en Internet: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.7c.Forensic_Profiling.pdf [consulta: 07 de agosto de 2017].

de normas complementarias en relación con las particularidades del contexto peculiar de la protección de datos en el sector de aplicación de la ley.

132. La Decisión en examen tenía por objeto proteger «*los derechos y libertades fundamentales*» de las personas cuando sus datos personales son tratados a los efectos de «*prevención*», «*investigación*», «*detección*» o «*enjuiciamiento*» de delitos o de «*ejecución de sanciones penales*» (artículo 1 - Objetivo y ámbito de aplicación). Su ámbito de aplicación cubría «*tanto al tratamiento automatizado como no automatizado, total o parcial de datos personales*» en archivos. Sin embargo, la Decisión no perjudicó en modo alguno a los intereses fundamentales de la seguridad nacional y actividades de inteligencia específicas en el ámbito de la seguridad nacional. Ahora bien, dado que el ámbito de la Decisión es la cooperación policial y judicial, sólo se aplicaba al intercambio de datos entre los Estados miembros, y no al tratamiento de datos a nivel nacional[532]. Aunque tal instrumento mejoró la situación de aquel momento, lo cierto es que este punto no fue uno de los más controvertidos[533], si no el más controvertido. Éste incluye el intercambio de información entre los Estados miembros, pero excluye cualquier forma de intercambio doméstico, un factor que escapa al control de una gran parte del intercambio de datos. A esto se añade la declaración explícita de que la Decisión «*no afectará a los intereses esenciales de seguridad del Estado ni a las actividades específicas de inteligencia en el sector de la seguridad del Estado*» (artículo 1, apartado 4). Esta Decisión, que se analizará más adelante, supone un

[532] Artículo 1 (Objetivo y ámbito de aplicación) de la DECISIÓN MARCO 2008/977/JAI: «*1. El objetivo de la presente Decisión Marco es garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea, garantizando al mismo tiempo un alto nivel de seguridad pública. 2. De conformidad con lo establecido en la presente Decisión Marco, los Estados miembros protegerán los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, cuando, para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales los datos personales: a) los Estados miembros los transmitan o hayan transmitido o los pongan o hayan puesto a disposición entre sí; b) los Estados miembros los transmitan o hayan transmitido a autoridades o sistemas de información creados en virtud del título VI del Tratado de la Unión Europea, o los pongan o hayan puesto a su disposición, o c) las autoridades o sistemas de información creados en virtud del Tratado de la Unión Europea o del Tratado constitutivo de la Comunidad Europea los transmitan o hayan transmitido a las autoridades competentes de los Estados miembros, o los pongan o hayan puesto a su disposición* (…)».

[533] Al acto de su adopción, el SEPD expresó tres críticas: «*the need to distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards; ensuring an adequate level of protection for exchanges with third countries according to a common EU standard; providing consistency with the first pillar's Data protection Directive 95/46/EC, in particular by limiting the purposes for which personal data may be further processed*». En EUROPEAN DATA PROTECTION SUPERVISOR - Press Release (2008). Este aspecto ha sido al centro de debate y ha visto persistir dos facciones opuestas dentro del Consejo de Europa, *vid*. «EU: Data protection proposal in a muddle - member states divided - three Council working parties discussing the draft measure», en *Statewatch News online*, 2006. Disponible en Internet: http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm [consulta: 09 de agosto de 2017].

primer paso en el necesario desarrollo de la dimensión de protección de las libertades y derechos en el seno de la cooperación judicial penal en la UE[534].

133. En cuanto al tratamiento de los datos personales, estaba previsto que los sujetos encargados respeten los principios de licitud, proporcionalidad y finalidad. Los datos personales, a excepción de algunos casos específicos, pueden ser recogidos por «*las autoridades competentes de los Estados miembros*», en el cumplimiento de determinadas obligaciones, solamente con «*fines determinados, explícitos y legítimos*», y sólo pueden utilizarse para el fin para el que han sido recogidos[535]. En la transmisión de datos, en principio, los datos personales recibidos de otro Estado miembro sólo podrán utilizarse para los fines para los que fueron proporcionados. Excepto en ciertos casos, pueden ser tratados para diferentes finalidades, tales como «*la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o para la ejecución de sanciones penales*» o para la prevención de amenazas graves a la seguridad pública[536]. Además, se reconocía una serie de derechos de la persona interesada al tratamiento de datos personales, como el derecho a la información, que los datos sean rectificados, eliminados o bloqueados y, por fin, pedir una indemnización en caso de daños causados por un tratamiento ilegal de datos personales[537]. Por último, obligaba a «*las autoridades competentes de los Estados miembros*» a que "adopten las medidas de seguridad necesarias para proteger los datos personales de cualquier tipo de tratamiento ilegal, así como la pérdida accidental, la alteración, divulgación o acceso no autorizado"[538]. En general, los interesados tendrán «*derecho a un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional*» de aplicación de la Decisión Marco de protección de datos[539].

---

[534] José Francisco ETXEBERRIA GURIDI (2009: 354).
[535] Artículo 3 (Principios de licitud, proporcionalidad y finalidad) de la DECISIÓN MARCO 2008/977/JAI.
[536] Artículo 11 (Tratamiento de datos personales transmitidos o puestos a disposición por otro Estado miembro), artículo 13 (Transferencia a autoridades competentes de terceros Estados y a organismos internacionales) y artículo 14 (Transmisión a particulares en los Estados miembros) de la DECISIÓN MARCO 2008/977/JAI.
[537] Artículo 16 (Información al interesado), artículo 18 (Derecho de rectificación, supresión o bloqueo) de la DECISIÓN MARCO 2008/977/JAI. El derecho de acceso que, aunque no es absoluto, ve su efecto en los Estados en la posibilidad de prever limitaciones en una serie de casos enumerados, aunque se establece que se deben tener en «*cuenta los intereses legítimos del interesado*» o ser necesarias y proporcionadas. A continuación, se pasa el derecho de rectificación, supresión y bloqueo, por un procedimiento que, sin embargo, deja a los Estados miembros un margen considerable sobre los procedimientos y, una vez más, las limitaciones reconocidas al derecho. Cuando el ejercicio de dichos derechos sea denegado, el interesado «*puede recurrir ante la autoridad nacional de control o los juzgados o tribunales competentes*» (artículo 17 - Derecho de acceso a los datos). Si la persona sufre «*daños y perjuicios como consecuencia del tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Decisión Marco, tendrá derecho a obtener reparación por los mismos del responsable del tratamiento o de otra autoridad competente de acuerdo con el Derecho nacional*» (artículo 19 - Derecho a reparación).
[538] Artículo 21 (Confidencialidad del tratamiento) y artículo 22 (Seguridad del tratamiento) de la DECISIÓN MARCO 2008/977/JAI.
[539] Artículo 20 (Vías de recurso) de la DECISIÓN MARCO 2008/977/JAI.

134. El marco legal que se ha descrito anteriormente, evidentemente, dejaba gran libertad a los Estados, impidiendo el logro de un alto nivel de protección de datos compartidos, y también, en consecuencia, imposibilitando en gran medida una relación de la confianza mutua entre las autoridades competentes necesaria para una cooperación eficaz[540]. Según el considerando 6 de la Decisión, las autoridades policiales debían cumplir con esta norma cada vez que transferían datos personales a otro Estado miembro para prevenir, investigar, detectar o perseguir un delito penal, y dejar a los Estados miembros la facultad de determinar con mayor precisión, a nivel nacional otros fines que deben considerarse incompatibles con el fin con el que se recopilaron inicialmente los datos personales. Las autoridades competentes adoptaban las medidas de seguridad necesarias para proteger los datos personales contra cualquier forma ilícita de tratamiento. Todos los datos personales recogidos, conservados y tratados, cumpliendo estrictamente condiciones fundamentales en el ámbito de la protección de datos, se pueden intercambiar en el marco de la cooperación policial y judicial en materia penal, especialmente con arreglo al principio de disponibilidad con las autoridades competentes de otro Estado miembro[541]. Este intercambio se basaba en normas claras que aumenten la confianza mutua entre las autoridades competentes y garanticen la protección de la correspondiente información, excluyendo toda discriminación respecto de esta cooperación entre los Estados miembros y, al mismo tiempo, garantizando el pleno respeto de los derechos fundamentales de la persona[542] (considerando 5). Con respecto a las autoridades nacionales, tanto en la Directiva de 1995 tanto en la Decisión Marco, se especificaban poderes para autoridades de protección de datos independientes. Sin embargo, una diferencia se observa en la Decisión donde no había ninguna referencia de un organismo de supervisión similar al Grupo de protección de datos del Articulo 29 reglado por la Directiva 95/46 (artículo 29 de la Directiva).

135. A pesar de la atención dedicada a la protección de los datos personales quedaban, de hecho, varios aspectos problemáticos, en particular, sobre el contexto de la aplicación de la

[540] Dichas autoridades son agencias u organismos de la UE, así como autoridades de los Estados miembros. La definición de «*autoridades competentes*» la encontramos en su artículo 2, letra h): «*los servicios u organismos creados en virtud de actos jurídicos adoptados por el Consejo al amparo del título VI del Tratado de la Unión Europea, así como las autoridades policiales, judiciales, aduaneras y otras autoridades competentes de los Estados miembros autorizadas por el Derecho nacional a tratar datos personales en el ámbito de la presente Decisión Marco*».

[541] Fernando MARTÍNEZ PÉREZ y María POZA CISNEROS (2013a).

[542] Cada Estado miembro deberá garantizar que una o más autoridades nacionales de supervisión independientes «*se encarguen en su territorio de asesorar y vigilar la aplicación de las disposiciones*» adoptadas con arreglo a la Decisión Marco de protección de datos. También entenderán de «*las solicitudes que cualquier persona le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales*» por parte de las autoridades competentes. Artículo 25 (Autoridades nacionales de control) de la DECISIÓN MARCO 2008/977/JAI.

Decisión abordaba la transmisión de datos entre los Estados miembros y no las operaciones de tratamiento que se realizan a nivel nacional[543]. Sobre este punto, algunos Países han mostrado dificultades a la hora de establecer, en la práctica, una diferencia entre el procesamiento transfronterizo y aquel a nivel nacional, destacando la complejidad de la aplicación de normas distintas a los mismos datos personales[544], lo que determina nuevas formas de discriminación y es, al mismo tiempo, claramente poco funcional y práctico[545].

136. Otro punto débil de la Decisión Marco fue la exclusión de determinados instrumentos sectoriales de la UE del marco de la Decisión[546] (considerando 39). Asimismo, excluía "taxativamente" de su ámbito de aplicación «*los intereses esenciales de seguridad del Estado*» así como «*a las actividades específicas de inteligencia en el sector de la seguridad del Estado*» (artículo 1, apartado 4). Especialmente, la Decisión Marco, como acto horizontal de protección de datos no afectó «*al conjunto pertinente de disposiciones de protección de datos*» de diferentes «*actos adoptados en virtud del título VI*» del TUE antes de la Decisión Marco[547], en particular en aquellos casos de tratamiento de datos por parte de

[543] Críticas han sido las observaciones formuladas por el SEPD en tres distinguidos dictámenes durante el proceso de aprobación de la Decisión Marco. *Vid*. *amplius*: DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (COM (2005) 475 final), *Diario Oficial de la Unión Europea*, C 47 de 25.2.2006, págs. 27–47. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52006XX0225(01) [consulta: 09 de agosto de 2017]; SEGUNDO DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, *Diario Oficial de la Unión Europea*, C 91 del 26.4.2007, págs. 9–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0426(02) [consulta: 09 de agosto de 2017]; TERCER DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, (2007/C 139/01), *Diario Oficial de la Unión Europea*, C 139 del 23.6.2007, págs. 1–10. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0623(01) [consulta: 09 de agosto de 2017]. También *vid*. Paul DE HERT and Rocco BELLANOVA (2009), «Data Protection in the Area of Freedom, Security and Justice: A System Still to be Fully Developed?», en *Briefing Paper*, Study requested by the European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs, Brussels, PE 410.692, págs. 5 y ss. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL-LIBE_NT(2009)410692_EN.pdf [consulta: 07 de agosto de 2017].

[544] INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES presentado de conformidad con el artículo 29, apartado 2, de la Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0012 [consulta: 07 de agosto de 2017].

[545] TERCER DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS; Paul DE HERT and Rocco BELLANOVA (2009).

[546] Cristina BLASI CASAGRAN (2015), «Límites del derecho europeo de protección de datos en el control de fronteras de la UE», en *Revista CIDOB d'Afers Internacionals*, núm. 111, pág. 136. ISSN:1133-6595.

[547] Considerando 39 de la DECISIÓN MARCO 2008/977/JAI. Criticas muy fuertes, llegaron también del Grupo de Trabajo del Artículo 29. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY - Working Party on Police and Justice (2009), The Future of Privacy. Joint contribution to the Consultation of the

«*Europol, Eurojust, el Sistema de Información de Schengen (SIS) y el Sistema de Información Aduanero (SIA)*» y sistema Prüm, «*ni a los que permiten a las autoridades de los Estados miembros acceder directamente a determinados sistemas de datos de otros Estados miembros*» (por ejemplo, los Acuerdos *PNR*) así como, del mismo modo, otros actos legislativos de la UE adoptados previamente que permiten el intercambio de información en el ámbito penal[548]. La Decisión no unificó, sin embargo, el régimen jurídico aplicable, sino que éste se complica cuando en su artículo 28 dispone, respecto a las actuaciones adoptadas antes de la entrada en vigor de la referida norma, que regulen «*el intercambio de datos personales entre los Estados miembros o el acceso de unas autoridades designadas de los Estados miembros a sistemas de información establecidos en virtud del Tratado constitutivo de la Comunidad Europea, establezca condiciones específicas respecto de la utilización de dichos datos por el Estado miembro receptor, estas primarán sobre las disposiciones de la presente Decisión Marco relativas al uso de los datos transmitidos o puestos a disposición por otro Estado miembro*»[549].

137. La Decisión Marco no distinguía entre las distintas categorías de personas a las que pertenecen los datos, como los sospechosos, los delincuentes, los testigos y las víctimas, para garantizar que sus datos se tratasen con garantías adecuadas[550].

138. En definitiva, la Decisión Marco 2008/977/JAI relativa a la protección de datos personales en la cooperación policial y judicial en materia penal no ofreció las garantías necesarias, ni jurídicas ni prácticas, para la protección efectiva del derecho a la protección de datos a nivel de la UE, sobre todo, porque se privilegió la aplicación de disposiciones de

European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009, 02356/09/EN, WP 168, págs. 4 y ss.

[548] Considerando 39 de la DECISIÓN MARCO 2008/977/JAI. Tampoco la norma se aplicaba a las disposiciones de protección de datos que «*rigen la transferencia automatizada de perfiles de ADN, datos dactiloscópicos y datos de los registros nacionales de matriculación de vehículos en virtud de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza*». En este sentido, el SEPD en su Dictamen de 2006, había expresado su preocupación por hincapié de la importancia de vigilar sobre el hecho que la Decisión Marco «*no propiciará la interconexión incondicional de bases de datos y, por ende, la creación de una red de bases de datos que sería difícil de supervisar*», y por lo tanto potencialmente muy perjudiciales para el objetivo de limitar los efectos de la transferencia y el tratamiento posterior de los datos. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2005).

[549] Artículo 28 (Relación con actos de la Unión adoptados previamente): «*Cuando algún acto, adoptado en virtud del título VI del Tratado de la Unión Europea antes de la fecha de entrada en vigor de la presente Decisión Marco y que regule el intercambio de datos personales entre los Estados miembros o el acceso de unas autoridades designadas de los Estados miembros a sistemas de información establecidos en virtud del Tratado constitutivo de la Comunidad Europea, establezca condiciones específicas respecto de la utilización de dichos datos por el Estado miembro receptor, estas primarán sobre las disposiciones de la presente Decisión Marco relativas al uso de los datos transmitidos o puestos a disposición por otro Estado miembro*».

[550] EUROPEAN DATA PROTECTION SUPERVISOR - Press Release (2008).

protección de datos de dichas bases de datos sobre la protección comprendida en la Decisión, así como a diferentes niveles de protección de datos en Estados miembros[551]. Esta consideración, además de ser deducida a partir del análisis de la Decisión, es evidente en comparación con la Directiva 95/46/CE antes analizada que, aun con las limitaciones resaltadas, aparece mucho más precisa y garantista[552]. Esto, a pesar de la base jurídica de la Directiva, era la armonización de la legislación en vista de la realización del mercado interior, y por lo tanto no es una disposición que tiene la protección del derecho a la protección de datos como objetivo de carácter central o principal[553].

139. Asimismo, el hecho de que la Decisión fuera esencialmente un instrumento *pre*-Lisboa, que debía lograr la unanimidad entre los Estados miembros y ajustarse al sistema de pilares, nos lleva a considerar necesario destacar que sus principios están redactados de una forma que casi podríamos decir que derivan en ciertos puntos en un tipo de aplicación voluntaria[554]. Por último, la protección de los derechos individuales, como el derecho a la información, el acceso, la rectificación o la eliminación de los datos personales, era inadecuada y daba prioridad no equilibrada a las necesidades del procesamiento de datos relacionado con la seguridad.

140. El diferente grado de garantía expresada por los dos instrumentos (Directiva y Decisión Marco) es mucho más relevante por el hecho de que la falta de seguridad en la recogida y tratamiento de datos puede, en el contexto de la cooperación policial, conducir a la violación de otros derechos y libertades fundamentales, tales como el derecho a la no

[551] Costanza DI FRANCESCO MAESA (2016), «Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)», en *Rivista Eurojus*. Disponible en Internet: http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/ [consulta: 07 de agosto de 2017].

[552] No obstante, las expectativas eran adoptar un sólido instrumento de protección de datos compatible con los principios establecidos en la Directiva 95/46/CE. De hecho, este fue el enfoque propuesto por la Comisión Europea en 2005. Tanto la estructura de la propuesta de Decisión Marco (con excepción de las formas específicas de tratamiento del Capítulo III que no tenía precedentes) como el enfoque del tema se redactaron siguiendo las líneas de la Directiva 95/46/CE. Paul DE HERT, Vagelis PAPAKONSTANTINOU and Cornelia RIEHLE (2008: 165).

[553] Por ejemplo, la Decisión Marco no incluye ningún artículo que prohíba el tratamiento de datos sensibles, sino que el propio artículo 6 establece que los datos relativos a la raza, política, creencias filosóficas o religiosas, participación en sindicatos, salud o vida sexual de una persona podrán tratarse siempre de que sea estrictamente necesario y bajo unas garantías adecuada, que no se especifican en ninguna forma. Además, aunque hay una referencia al hecho de que el tratamiento debe ser considerado necesario, carece de cualquier mención de proporcionalidad.

[554] Otro aspecto crítico de la Decisión Marco fue su naturaleza. En este sentido, la Comisión no tenía medios para obligar a los Estados miembros a que cumplieran con ella.

discriminación y la libertad de movimiento[555]. Este fenómeno, sin duda, se amplifica gracias al progreso tecnológico, que tiene el efecto de aumentar aún más las posibilidades de violación.

141. Todos estos problemas hacen de la Decisión Marco un instrumento jurídico tan débil que no ha logrado garantizar un conjunto armonizado de reglamentaciones y reforzar las libertades civiles en Europa[556]. Las debilidades de la Decisión Marco muestran claramente la falta de una norma común de protección de datos efectiva en el *ex* tercer pilar y que esta ausencia es importante.

142. Por consiguiente, los nuevos desafíos han comprometido particularmente las instituciones europeas en el logro de este ambicioso objetivo, como queda atestiguado por la adopción del conjunto de medidas reguladoras sobre esta materia, consistente en el Reglamento del Parlamento Europeo y del Consejo n. 679/2016 (Reglamento General de Protección de Datos) y la Directiva del Parlamento Europeo y del Consejo n. 680/2016, que han sustituido respectivamente la Directiva 95/46/CE y la Decisión Marco 2008/977/JAI[557]. Por cuánto concierne al nuevo marco regulatorio para la prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, se decidió emplear el instrumento de la Directiva para introducir una importante revisión: en estas materias el legislador europeo ha preferido dejar un margen más amplio de discrecionalidad de los Estados miembros. Así pues, la diferencia entre un derecho fundamental que debe ser garantizado en todo el territorio y para todos los ciudadanos, y la exigencia de seguridad, un interés colectivo, que se considera como fundamental, pero territorialmente diferenciable, por las decisiones soberanas de los Estados individuales que tengan en cuenta las especificidades diferentes, parece también surgir en cuanto a los instrumentos utilizados para la regulación de sus respectivas áreas.

143. El nuevo marco regulador tiene como objetivo satisfacer "la necesidad de establecer un marco jurídico más sólido y coherente que, junto con medidas eficaces de aplicación, les

[555] TJUE (Gran Sala), *Comisión de las Comunidades Europeas contra Reino de España*, asunto C-503/03, sentencia de 31 de enero de 2006.
[556] Paul DE HERT, Vagelis PAPAKONSTANTINOU and Cornelia RIEHLE (2008: 122).
[557] Ignacio COLOMER HERNANDEZ (2015), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Pamplona, Aranzadi, págs. 851. ISBN: 978-84-9059-917-4.

garantice a las personas el control de sus datos personales, lo que refuerza la misma seguridad jurídica y operativa de los agentes económicos y las autoridades públicas"[558].

[558] Didier BIGO, Sergio CARRERA, Gloria GONZÁLEZ FUSTER, *et ál*. (2011), *Towards a New EU Legal Framework for Data Protection and Privacy. Challenges, Principles and the Role of the European Parliament*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, págs. 157. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/453216/IPOL-LIBE_ET(2011)453216_EN.pdf [consulta: 16 de enero de 2016].

CAPÍTULO III

LOS SISTEMAS DE GESTIÓN DE LA INFORMACIÓN DEL ESPACIO EUROPEO DE LIBERTAD, SEGURIDAD Y JUSTICIA Y LA PROTECCIÓN DE DATOS

1. Planteamiento general de la relevancia de la protección de datos en el ELSJ de la Unión Europea

1. Durante las últimas décadas han coincidido en Europa una serie de fenómenos como el incremento de la amenaza terrorista o las crisis migratorias del Mediterráneo, que han derivado en un incremento de las medidas de seguridad y orden público, intensificándose así su tensión con el derecho fundamental a la protección de los datos personales. Desde hace años, la UE ha adoptado numerosas medidas a través de instrumentos y políticas para la gestión del Espacio de Libertad, Seguridad y Justicia (ELSJ)[559], que han conllevado (y siguen conllevando) el tratamiento masivo de datos personales tanto de ciudadanos europeos como no europeos, con el fin de hacer posible el intercambio mutuo de los datos e información entre las bases de datos de las autoridades nacionales y europeas interesadas en estos datos, y, asimismo, su transferencia a terceros países.

2. La implementación del espacio de libre circulación en el interior de las fronteras de la Unión Europea experimentó un salto cualitativo con el Tratado de Lisboa que condujo a una progresiva ampliación de las competencias europeas en el que, hasta entonces, fuera el tercer pilar de la Unión. Se modificó la base jurídica y se incrementaron las atribuciones de las instituciones comunitarias en dicho ámbito. Este impulso, sumado a otras iniciativas intergubernamentales que tratan de avanzar hacia respuestas comunes a riesgos compartidos,

[559] «*En los años ochenta del siglo pasado la UE empezó a recoger datos de personas que llegaban de terceros países a territorio europeo para controlar los flujos migratorios. Sin embargo, los atentados terroristas del 11-S de 2001, Madrid el 11 de marzo de 2004 y Londres el 7 de julio de 2005, propiciaron una extensión progresiva del uso de tal información, originalmente sólo prevista para controlar la inmigración, para fines policiales*». Cristina BLASI CASAGRAN (2015: 127). «*A partir de estos hechos, la seguridad de la Unión y de los Estados miembros pasa a tener un carácter prioritario en las políticas que se desarrollaron, dándole especial énfasis a la prevención y represión del terrorismo (pero sin descuidar otros ámbitos importantes, como la delincuencia organizada, la migración ilegal, la trata y la introducción clandestina de seres humanos en los países de la Unión)*». Alejandro Luis GACITÚA ESPÓSITO (2014: 153). Una visión progresiva del trabajo que desarrollan las instituciones y agencias UE, con el objetivo de asegurar un ELSJ sin fronteras interiores donde los ciudadanos podamos disfrutar de nuestros derechos y libertades de forma segura, *vid*. Ángeles GUTIÉRREZ ZARZA (2017), «Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ en 2016», en *Diario La Ley*, Sección Tribuna, Editorial Wolters Kluwer, núm. 8904. Disponible en Internet: http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras-prueba-electronica-encriptado- [consulta: 30 de enero de 2017].

ha dado lugar a la creación de un complejo esquema institucional en materia de seguridad derivado de una serie de acuerdos internacionales que prevén la creación de organismos y agencias con un alto grado de autonomía pero sin un marco jurídico claro dentro del seno de la Unión Europea[560], lo que ha llevado la necesidad de establecer mecanismos de control democrático para asegurar que sus acciones recaen dentro de sus respectivos mandatos y respetan los derechos y libertades fundamentales de la Unión. También hay que recordar que todas estas cuestiones se plantean en un ámbito de la cooperación internacional y no de integración, por lo que a las tensiones que surgen naturalmente entre las medidas de seguridad y orden público y la protección de los derechos y las libertades fundamentales, se añade el hecho de que se trata de una política caracterizada por su "geometría variable" entre los diferentes Estados[561], contribuyendo así a crear fuertes incertidumbres en el ámbito de la protección efectiva de los datos personales y con respecto control sobre el uso que se haga de los mismos.

3. Esta ausencia de un marco jurídico estable y definido resulta especialmente grave en lo que respecta a los instrumentos europeos de gestión de la información en el ELSJ, "que se utilizan para el manejo de información personal con fines represivos o de gestión de la migración", ya que, por su finalidad, son sistemas que se ocupan de cuestiones especialmente sensibles, relacionadas con la seguridad colectiva e individual y los derechos de las personas pero que implican la utilización de datos de carácter personal. Debe tenerse en cuenta que muchos de estos instrumentos «*fueron originalmente creados para fines de control fronterizo*»[562], si bien derivaron en mecanismos para el control del orden público y la seguridad ciudadana con carácter general. «*Este cambio de finalidad fue consecuencia de los atentados del 11-S, ya que antes del 2001 existían muy pocos sistemas europeos para el*

[560] *Vid*. DECISIÓN ADOPTADA DE COMÚN ACUERDO POR LOS REPRESENTANTES DE LOS GOBIERNOS DE LOS ESTADOS MIEMBROS REUNIDOS A NIVEL DE JEFES DE ESTADO O DE GOBIERNO RELATIVA A LA FIJACIÓN DE LAS SEDES DE DETERMINADOS ORGANISMOS Y SERVICIOS DE LAS COMUNIDADES EUROPEAS Y DE EUROPOL, *Diario Oficial*, n° C 323 de 30/11/1993, págs. 0001 - 0005.

[561] Por ejemplo, el Reino Unido e Irlanda, de hecho, han negociado, y todavía tienen, la posibilidad de asociarse a cada medida. Estos países tienen un acceso parcial al SIS, si bien existen estados fuera de la UE que han firmado el Acuerdo de Schengen y, por lo tanto, están plenamente implicados (Islandia, Liechtenstein, Noruega y Suiza). En este marco se añade también Dinamarca, que tiene una situación similar a la del Reino Unido e Irlanda, con la posibilidad de ejercer el "*opt-out*" en las medidas de desarrollo del Acuerdo. Los ámbitos regulatorios de SIS II, VIS y EURODAC se caracterizan por lo mismo, es decir, Irlanda y el Reino Unido forman parte de EURODAC, pero sólo participan parcialmente en el SIS II y no participan en el VIS, mientras que Dinamarca participa en los tres sistemas con arreglo a una base jurídica diferente. Por otra parte, Países no pertenecientes a la UE como Islandia, Noruega, Suiza y Liechtenstein, participan o participarán en la ejecución, aplicación y desarrollo del acervo de Schengen y, por tanto, participan tanto en el SIS II como en el VIS. *Vid*. *amplius* Mariona ILLAMOLA DAUSÀ (2015), «EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE», en *Revista CIDOB d'Afers Internacionals*, núm. 111, pág. 108.

[562] Cristina BLASI CASAGRAN (2015: 128).

intercambio de datos de inmigrantes accesibles a las autoridades policiales»[563] que posteriormente, se han multiplicado y han dado lugar a un complejo panorama[564]. Los sistemas de intercambio de información son, por lo tanto, uno de los principales instrumentos que se utilizan para asegurar la aplicación del ELSJ, pero al mismo tiempo son, en muchos casos, incompatibles con el principio de limitación de la finalidad de los datos personales reconocido en la normativa de protección de datos europea[565].

4. Las instituciones europeas, en una comunicación de la Comisión al Parlamento y al Consejo, subrayan que «*la existencia de sistemas de información a gran escala implica riesgos potenciales para la intimidad, que deben preverse y abordarse convenientemente. La recopilación y el uso de datos personales en estos sistemas tiene repercusiones en el derecho a la intimidad y la protección de los datos personales*», consagrados como derechos fundamentales en la CDFUE y en las constituciones de los Estados miembros. Por lo tanto, «*todos los sistemas deben ajustarse a los principios de protección de datos y a los requisitos de necesidad, proporcionalidad, limitación de la finalidad y calidad de los datos*»[566], con reglas claras y comunes para el tratamiento de los

[563] Cristina BLASI CASAGRAN (2015: 128).

[564] La Comisión Europea ha intentado en varias ocasiones clasificar sus propias actividades en estos ámbitos: COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia, COM/2010/0385 final, Bruselas, 20.7.2010. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0385 [consulta: 06 de marzo de 2015]. Según esta Comunicación, la Comisión clasifica los instrumentos en: «*1) Instrumentos de la UE para mejorar el funcionamiento del espacio de Schengen y de la unión aduanera: Sistema de Información de Schengen (SIS); Sistema de Información de Schengen de segunda generación (SIS II); EURODAC; Sistema de Información de Visados (VIS); Información Previa sobre Pasajeros (API); Convenio de Nápoles II; Sistema de Información Aduanero (SIA). 2) Instrumentos de la UE para prevenir y combatir el terrorismo y otras formas graves de delincuencia transfronteriza: Decisión Prüm; Directiva sobre conservación de datos de 2006; Sistema de Información Europeo de Antecedentes Penales (ECRIS); Unidades de Información Financiera; Organismos de Recuperación de Activos. 3) Agencias y organismos de la UE encargados de ayudar a los Estados miembros a prevenir y combatir las formas graves de delincuencia transfronteriza: Oficina Europea de Policía (Europol); Unidad Europea de Cooperación Judicial (Eurojust). 4) Acuerdos internacionales para prevenir y combatir el terrorismo y otras formas graves de delincuencia transnacional: Registro de Nombres de Pasajeros (PNR); Programa de seguimiento de la financiación del terrorismo*». *Vid* también, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4.11.2010. Disponible en Internet: http://ec.europa.eu/health/data_collection/docs/com_2010_0609_es.pdf [consulta: 10 de enero de 2015]; COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Refuerzo de la cooperación en materia de aplicación de la ley en la UE: el Modelo Europeo para el Intercambio de Información (EIXM), COM/2012/0735 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0735 [consulta: 06 de marzo de 2015].

[565] Según la opinión del Grupo de Trabajo del Artículo 29, en ARTICLE 29 DATA PROTECTION WORKING PARTY (2013c: 68 y ss.).

[566] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, Bruselas, 6.4.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016DC0205 [consulta: 23 de julio de 2017]. La comunicación de la Comisión

datos, sin perjuicio de que sean operativos para el desarrollo de la actividad de seguridad pública tanto a nivel interno como europeo. Esto nos lleva a que la existencia a nivel europeo, de una serie de sistemas que permiten la obtención, el procesamiento y la creación de bases de datos con los consiguientes canales de intercambio y la conexión entre la información, requiere una especial atención a la cuestión de la protección de datos contenida en los mismos. La elaboración de una normativa uniforme de protección de datos personales, se considera aún más necesaria ante la creación de bases de datos que permiten la interconexión y el flujo de información entre distintos actores y países, por lo que esta normativa debe garantizar una regulación uniforme de la protección de datos bajo el doble aspecto de la seguridad pública y del derecho subjetivo a la privacidad de los titulares de los datos[567].

5. Los sistemas de intercambio de información que se utilizan a escala europea dentro de la Unión para el desarrollo de la política ELSJ, y que proporcionan a las autoridades responsables de la seguridad y del orden público información pertinente sobre las personas, son muy diversos y pueden clasificarse en función de diferentes criterios[568]. En todo caso no se trata de un conjunto de sistemas perfectamente ordenado y sistemático, sino que la arquitectura de los sistemas de gestión de datos de la Unión Europea es el resultado de un proceso acumulación, por lo que cada uno de los sistemas tienen «*sus propios objetivos, finalidades, bases jurídicas, grupos de usuarios y contexto institucional*»[569].

6. Entre los diversos sistemas de información que existen dentro del ELSJ se procede, a continuación, al análisis de aquellos que, según nuestra opinión, tienen mayores

también aclara que es necesario «*establecer salvaguardias para garantizar los derechos de los interesados en relación con la protección de su vida privada y sus datos personales. Los datos sólo deberán conservarse durante el tiempo que sea necesario para la finalidad para la que fueron recogidos. Deben preverse mecanismos que garanticen una gestión del riesgo adecuada y una protección efectiva de los derechos de los interesados*».

[567] La nueva reforma dictada por las instituciones europeas en el 2016 (Reglamento y Directiva), mantiene, como veremos, excepciones a su ámbito de aplicación, reduciendo su original intento homogeneizador de niveles de protección de los datos personales en todos los ámbitos del Derecho de la Unión y su aplicabilidad del marco general (*vid*. Capítulo V).

[568] En este sentido, *vid*. Lucia MUSSELLI (2013), «Alcune prime considerazioni sui sistemi di scambio di informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti», en *Research Paper Centro Studi sul Federalismo*, pág. 7. Disponible en Internet: http://www.csfederalismo.it/attachments/article/832/CSF-RP_Musselli_Sistemi_di_scambio_di_informazioni_maggio2013.pdf [consulta: 15 de marzo de 2015]. De acuerdo con otra doctrina en cambio los sistemas de intercambio de información, entendidos como herramientas de política sobre todo como "instrumentos de capacidad" se distinguen en función de su relevancia "interna" (como Eurodac, SIS y VIS) o "externa" (como Europol-*USA Agreements* y *PNR*) a la Unión. En Thierry BALZACQ (2008), «The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies», en *JCMS: Journal of Common Market Studies*, volume 46, issue 1, pág. 83.

[569] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

implicaciones en el intercambio de datos personales con fines de seguridad pública y que, en el momento actual, se encuentran en un proceso de reformas por parte de las instituciones europeas para abordar de manera más eficaz los nuevos desafíos que se plantean a la seguridad interior[570].

7. Los tres principales sistemas de información centralizados desarrollados para el control de la circulación de las personas en la Unión Europea son: «*el Sistema de Información de Schengen (SIS) con un amplio espectro de descripciones de personas y objetos*»; «*el Sistema de Información de Visados (VIS) con datos sobre visados para estancias de corta duración*»; y «*el Sistema Eurodac, con datos relativos a impresiones dactilares de solicitantes de asilo y nacionales de terceros países que han cruzado las fronteras exteriores de forma irregular*»[571]. Los sistemas mencionados «*son complementarios y, con la excepción del SIS, están principalmente destinados a los nacionales de terceros países*» y «*apoyan a las autoridades nacionales en la lucha contra la delincuencia y el terrorismo*», en particular en el caso del SIS que es el instrumento de intercambio de información más utilizado en la actualidad[572]. Los tres principales sistemas informáticos ahora comentados, son gestionados por la nueva Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (en adelante, *eu-LISA*), que contribuye a la aplicación de las políticas de justicia y asuntos de interior de la UE mediante la gestión operativa de sistemas informáticos de gran magnitud[573].

---

[570] Los Estados miembros de la UE han podido utilizar sistemas de recopilación e intercambio de información como Schengen, Eurodac, Prüm y otros, que han experimentado mejoras significativas. Sin embargo, aún queda mucho por mejorar atendiendo a los recientes ataques terroristas (Barcelona, Turku, Londres, Estocolmo y Berlín), que hubieran exigido un intercambio más efectivo y rápido de información.

[571] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[572] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final. Además de estos sistemas existentes, la Comisión propone «*crear un cuarto sistema centralizado de gestión de las fronteras, el Sistema de Entradas y Salidas (SES), que se espera entre en funcionamiento en 2020, dirigido asimismo a los nacionales de terceros países.* (…) *Otros instrumentos existentes para la gestión de fronteras son la base de datos de Interpol sobre documentos de viaje robados y perdidos (DVRP) y el sistema de información anticipada sobre los pasajeros (API), que recopila información sobre los pasajeros antes de los vuelos con destino a la UE. Estos instrumentos son pertinentes para los ciudadanos de la UE y los nacionales de terceros países*».

[573] La Agencia, sustituye y sucede a la Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, creada por el Reglamento (UE) n. 1077/2011. *Vid*. REGLAMENTO (UE) 2018/1726 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de noviembre de 2018 relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n. 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n. 1077/2011. Según lo establecido en el artículo 1 del mismo Reglamento, la "gestión operativa" consistirá «*en todas las funciones necesarias para el mantenimiento del funcionamiento de los*

8. Por otra parte, y «*específicamente con fines policiales, de investigación penal y cooperación judicial, la UE ha desarrollado instrumentos descentralizados para el intercambio de información*»[574], entre ellos destaca la Convención de Prüm[575] que sirve de marco para el intercambio de ADN, impresiones dactilares y datos de matriculación de vehículos[576].

9. Asimismo, se han establecido agencias y organismos europeos para asistir a los Estados miembros de la UE en la prevención y la lucha de la delincuencia transfronteriza grave, como la Oficina Europea de Policía (Europol)[577], en cuyo seno se prevé el «*intercambio de información entre las autoridades policiales nacionales como eje de información criminal de la UE*»[578].

10. En cuanto a la cooperación con terceros países para prevenir y combatir el terrorismo y otras formas de delincuencia transnacional, existe «*un conjunto suplementario de sistemas de tratamiento de datos personales que se desarrolla en los Estados miembros y es el registro de nombres de los pasajeros*» (en inglés, *Passenger Name Record - PNR*). Los datos *PNR* consisten en información sobre pasajeros de aerolíneas facilitada en el momento de la

sistemas informáticos de gran magnitud de conformidad con las disposiciones específicas aplicables a cada uno de ellos, incluida la responsabilidad de las infraestructuras de comunicación que utilicen. Esos sistemas informáticos de gran magnitud no intercambiarán datos ni permitirán compartir información o conocimientos, salvo que se disponga de manera específica en un acto jurídico de la Unión».

[574] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[575] *Amplius* Teresa FREIXES SANJUÁN (2007), «Protección de datos y globalización. La Convención de Prüm», en *Revista de derecho constitucional europeo*, núm. 7, págs. 11 y ss. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2492884 [consulta: 19 de octubre de 2015].

[576] Con fines policiales, de investigación penal y cooperación judicial, la UE ha desarrollado otro instrumento descentralizado para el intercambio de información: «*el Sistema Europeo de Información de Antecedentes Penales (ECRIS) para el intercambio de información sobre antecedentes penales nacionales. ECRIS permite el intercambio de información, a través de una red segura, sobre las condenas anteriores pronunciadas contra una persona determinada por los órganos jurisdiccionales penales en la Unión Europea. Las solicitudes se basan principalmente en información de identificación alfanumérica, aunque es posible el intercambio de datos biométricos*». COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[577] La Unión Europea para intensificar la cooperación en la lucha contra la delincuencia, el Consejo creó Eurojust, órgano de la Unión competente en investigaciones y actuaciones relativas a la delincuencia grave que afecta al menos a dos Estados miembros. Su papel es promover la coordinación entre autoridades competentes de los distintos Estados miembros y facilitar la cooperación judicial entre ellos. Eurojust tiene también que desempeñar un papel esencial en materia de lucha contra el terrorismo. *Vid*. DECISIÓN DEL CONSEJO, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (2002/187/JAI), *Diario Oficial de la Unión Europea*, L 063 de 06/03/2002, págs. 0001 – 0013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32002D0187 [consulta: 02 de agosto de 2017].

[578] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

reserva y la facturación[579]. Como se analizará de forma más extensa en el estudio sobre este sistema de tratamiento de datos personales que figura en el capítulo siguiente, la Comisión ha firmado los acuerdos *PNR* con Estados Unidos, Australia y Canadá. También este sistema ha sido objeto de un *leading case* del TJUE que se analizará más adelante.

11. Desde esta premisa, nos enfrentamos a «*un panorama complejo de sistemas de información gestionados de forma diferente a escala de la UE*». También tenemos que poner de relieve que «*no todos los Estados miembros están conectados a todos los sistemas existentes*». La dificultad existente del acceso a los sistemas de información de la Unión Europea podría reducirse estableciendo «*una interfaz única de búsqueda a escala nacional que respete los diferentes fines del acceso*»[580]. Como consecuencia, la complejidad de la estructura de gestión de datos de la Unión Europea en el ELSJ se destaca por su falta de unidad[581]. Podemos concluir que todo esto es consecuencia de los diferentes contextos institucionales, jurídicos y políticos de los diferentes países en los que se han desarrollado estos sistemas de información. De hecho, «*la información se almacena por separado en diferentes sistemas que tampoco suelen estar interconectados*». Tampoco hay coherencia entre «*las bases de datos y existen divergencias de acceso a los datos por parte de las autoridades pertinentes*»[582]. En este sentido, podemos afirmar que no hay utilidad en contar con todos estos sistemas si quedan aislados entre sí[583].

[579] Se trata de información más invasiva en relación con el itinerario del pasajero, la emisión de billete, informaciones de contacto, los agentes de viajes, forma de pago, información sobre el equipaje. Estos datos permiten identificar a las personas que no sean sospechosas antes, gracias a controles cruzados: son herramientas de inteligencia criminal y lucha contra el terrorismo. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[580] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final. «*Con sujeción a las disposiciones específicas del Protocolo núm. 22 por lo que respecta a Dinamarca, y los Protocolos núm. 21 y 36 por lo que respecta al Reino Unido e Irlanda, y las respectivas Actas de Adhesión*».

[581] Emanuele BONINI (2017), «Troppi database europei e pochi soldi per la sicurezza delle reti, l'Ue vuole più cybersecurity», en *Eunews*. Disponible en Internet: http://www.eunews.it/2017/06/29/troppi-database-europei-e-pochi-soldi-per-la-sicurezza-delle-reti-lue-vuole-piu-cybersecurity/88978 [consulta: 11 de agosto de 2017].

[582] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[583] *Vid*. *amplius*, Jesús Ángel FUENTETAJA PASTOR (2006), «Las agencias europeas de la cooperación policial y judicial», en *Revista de Derecho de la Unión Europea*, núm. 10, págs. 51-93. Disponible en Internet: http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:19805&dsID=AgEuCoPol.pdf [consulta: 24 de enero de 2015]; Franziska BOEHM (2012), «Information Sharing in the Area of Freedom, Security and Justice – Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems», en Serge GUTWIRTH, Ronald LEENES, Paul DE HERT, Yves POULLET (eds.), *European Data Protection: In Good Health?*, Dordrecht, Springer, págs. 143-183; Montserrat PI LLORENS y Esther ZAPATER DUQUE (coord.) (2014), *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia*, Madrid, Editorial Marcial Pons, págs. 218; Cristina BLASI CASAGRAN y Mariona ILLAMOLA DAUSÀ (coord.) (2016), *El control de las agencias del Espacio de Libertad, Seguridad y Justicia. Contrapeso necesario a su autonomía*, Madrid, Editorial Marcial Pons, págs. 210.

12. A la luz de las consideraciones preliminares expuestas, el uso de bases de datos a gran escala se convierte así en un elemento clave de los sistemas de intercambio de información a nivel europeo dentro del ELSJ y en la gestión de la información estructurada[584]. Por tanto, se hace necesaria llevar a cabo un análisis, sólo de algunas peculiaridades, de la normativa específica que regula estos sistemas de información, prestando especial atención a las disposiciones sobre datos personales, para comprobar cómo se garantiza la privacidad de las personas cuyos datos personales pueden estar a disposición de sujetos y organizaciones dentro y fuera de la UE, convirtiéndose así en un aspecto fundamental de instituciones específicas para la gestión del ELSJ, sobre todo debido a una efectiva particularidad de sus normas que justifica su excepción del régimen general de protección de datos, si bien las respectivas normas de protección de datos de estos instrumentos no coinciden entre ellos.

13. En resumen, el presente Capítulo intenta reflexionar sobre la forma en que los sistemas de información de la Unión Europea, intercambiando datos entre los Estados miembros y las autoridades competentes nacionales y de la Unión Europea, «*pueden reforzar la seguridad interior y la gestión de las fronteras, sobre la base de las importantes sinergias*» entre ellas, desarrollando acciones nuevas y complementarias para abordar las carencias[585], sin comprometer los valores y las libertades fundamentales de la UE. El objetivo principal es garantizar que las autoridades policiales, aduaneras y judiciales competentes cuenten sistemáticamente con la información necesaria para el desempeño de sus funciones, manteniendo al mismo tiempo un equilibrio con respecto a los derechos a la privacidad, la protección de datos y otros derechos fundamentales[586].

---

[584] Sobre las modalidades de funcionamiento, disciplina y de la evolución normativa de las principales bases de datos centralizadas de la Unión Europea, vid. Federico DECLI, Gabriella MARANDO (2009), «Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia», en Francesco PERONI, Mitja GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT - Edizioni Università di Trieste, págs. 101-138. Disponible en Internet: http://www.openstarts.units.it/dspace/handle/10077/3351 [consulta: 14 de marzo de 2016].

[585] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[586] ¿Con qué instrumentos se lleva a cabo la lucha contra el terrorismo en el espacio de la UE? ¿Se garantiza la protección y la efectividad de los derechos humanos por parte de los Estados? A estas preguntas, parece responder la investigación de Piotr Bakowski y Wouter Van Ballegooij, encargados por el departamento de investigación del Parlamento Europeo. La investigación, después de un examen de los instrumentos internacionales y de los actos adoptados a nivel universal y regional, lleva a cabo una evaluación de las medidas implementadas por la Unión Europea con un análisis *ex post* de los resultados conseguidos. Un factor esencial es la cooperación judicial, que a menudo tropieza con obstáculos de los Estados, incluso en áreas clave como la adquisición e intercambio de datos. Una cosa es cierta: la lucha contra el terrorismo debe llevarse a cabo a gran escala, desde intervenciones para prevenir el reclutamiento y la radicalización hasta bloquear el flujo de dinero que va a financiar grupos terroristas, pero siempre respetando los derechos humanos. También la investigación hace una evaluación de los costos del terrorismo, que se pondera por 185 mil millones de producto interno bruto en toda la Unión Europea. *Amplius*, Wouter VAN BALLEGOOIJ and Piotr

14. La Unión Europea se enfrenta al «*desafío de crear una arquitectura de gestión de datos más sólida e inteligente, respetando plenamente los derechos fundamentales, en particular la protección de los datos personales y el principio de limitación de la finalidad*». Los Estados miembros deben hacer «*pleno uso de los sistemas de información existentes y establecer las conexiones técnicas necesarias con todos los sistemas de información y bases de datos, en consonancia con sus obligaciones jurídicas*». Se destaca además «*la necesidad de mejorar la interoperabilidad de los sistemas de información como objetivo a largo plazo*». Por lo tanto, el reto de la Unión Europea «*debe ser desarrollar una estrategia común para hacer más eficaz y eficiente la gestión de datos en la UE, a fin de proteger mejor sus fronteras exteriores y reforzar su seguridad interior, respetando plenamente, en particular, a los derechos fundamentales, concretamente el derecho a la protección de los datos personales*»[587].

15. Por último, como afirma el TFUE, la Unión constituye un ELSJ «*dentro del respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicas de los Estados miembros*»[588]. Por consiguiente, «*las medidas legislativas que se adopten en la consagración de dicho Espacio deben respetar los derechos fundamentales de las personas que se encuentran dentro de la Unión* (…) *respetando los derechos y libertades fundamentales de las personas, y en particular, su privacidad y datos personales*»[589].

2. La protección de datos personales y seguridad nacional en el Espacio Schengen: el Sistema de Información de Schengen (SIS)

16. La necesidad de equilibrar la realización del mercado interior con una cooperación más estrecha en materia de seguridad, ha sido fuertemente sentida por algunos Estados europeos que, incluso antes de la firma del Tratado de Maastricht, decidieron empeñarse recíprocamente en un acuerdo externo a normativa constitutiva de la UE, a través de la creación de la zona de Schengen. Esa cooperación reforzada asimétrica, se inició el 14

BAKOWSKI (2018), *The Cost of Non-Europe in the fight against terrorism*, Brussels, European Added Value Unit - EPRS | European Parliamentary Research Service, PE 621.817, págs. 218. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621817/EPRS_STU(2018)621817_EN.pdf [consulta: 02 de septiembre de 2018].

[587] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[588] Artículo 67 (antiguo artículo 61 TCE y antiguo artículo 29 TUE), apartado 1, del TFUE.

[589] Alejandro Luis GACITÚA ESPÓSITO (2014: 151).

de junio de 1985 mediante el Acuerdo de Schengen[590] entre Alemania, Bélgica, Francia, Países Bajos y Luxemburgo relativo a la supresión gradual de controles en las fronteras interiores y a la creación de una única frontera exterior, que fue reforzado especialmente mediante el Convenio de Aplicación del Acuerdo Schengen (en adelante, CAAS)[591] de 19 de junio de 1990, que entró en vigor en 1995.

17. El Acuerdo de Schengen, firmado en Luxemburgo, constituye uno de los pasos más importantes en la historia de la construcción de la Unión Europea (UE)[592] y también, aunque en forma indirecta, en la evolución del derecho a la protección de los datos de carácter personal.

18. El Espacio Schengen representa un territorio, formado por los Estados signatarios, donde esté garantizada la libre circulación de las personas y, al mismo tiempo, se ha incrementado la cooperación y las relaciones entre autoridades policiales de los Estados miembros[593] y las autoridades judiciales para contrarrestar la amenaza a la seguridad pública que pueda derivar de la apertura de fronteras, reforzando los controles fronterizos en las fronteras exteriores del Espacio Schengen[594].

---

[590] *Vid*. «El espacio y la cooperación Schengen», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l33020 [consulta: 15 de enero de 2016]. Todos los países que participan en la cooperación Schengen no son miembros del Espacio Schengen: a) no deseaban suprimir los controles en sus fronteras; b) no reúnen todavía las condiciones requeridas para aplicar el acervo Schengen. *Vid*. al respecto, Adán Carrizo GONZÁLEZ-CASTELL (2008), «Instrumentos de asistencia policial en la Unión Europea: de Schengen a las estructuras orgánicas de cooperación policial», en Lorenzo M. BUJOSA VADELL, María del Carmen CALVO SÁNCHEZ (coord.), *Hacia un verdadero Espacio Judicial Europeo*, 1ª ed., Granada, Comares, págs. 159-195.

[591] ACERVO DE SCHENGEN - CONVENIO DE APLICACIÓN DEL ACUERDO DE SCHENGEN de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, *Diario Oficial de la Unión Europea*, L 239 de 22/09/2000, págs. 0019 – 0062. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):ES:HTML [consulta: 11 de enero de 2016]. Sobre el origen y desarrollo del Espacio Schengen, *vid*.: José Manuel LUQUE GONZÁLEZ (2004), «Schengen. Un espacio de libertad, seguridad y justicia», en *Revista de derecho: División de Ciencias Jurídicas de la Universidad del Norte*, núm. 21, págs. 139-149. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2347493 [consulta: 03 de febrero de 2016]; María del Carmen GUERRERO PICÓ (2006: 120-127); Raquel CASTILLEJO MANZANARES (2013), «Espacio Schengen», en Miguel CARMONA RUANO, Ignacio U. GONZÁLEZ VEGA, Víctor MORENO CATENA (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 267-319. Disponible en Internet: https://e-archivo.uc3m.es/handle/10016/18330 [consulta: 18 de enero de 2016].

[592] *Vid*. SERVIZIO STUDI DEL SENATO (2017), «Lo spazio Schengen e la sicurezza interna dell'Unione europea», en *Note su atti dell'Unione europea*, núm. 109, pág. 1. Disponible en Internet: http://www.senato.it/service/PDF/PDFServer/BGT/01022061.pdf [consulta: 03 de agosto de 2017].

[593] Antonio M. DÍAZ, Miguel REVENGA SÁNCHEZ, Óscar JAIME JIMÉNEZ y Rafael MARTÍNEZ MARTÍNEZ (2005), «Marco teórico para el análisis de la cooperación europea en materia de inteligencia», en *VIII Congreso de la Asociación de Ciencia Política y de la Administración*, Madrid, págs. 24-31. Disponible en Internet: http://www.aecpa.es/uploads/files/congresos/congreso_07/area03/GT09/DIAZ-Antonio.pdf [consulta: 04 de agosto de 2017].

[594] *Vid*. ampliamente Raquel CASTILLEJO MANZANARES (2013: 267-303).

19. El Acuerdo de Schengen, sin embargo, prevé la posibilidad de no aplicar el sistema de libre circulación de personas[595]. El artículo 2, apartado 2, del CAAS, especifica la posibilidad para los Estados miembros de reintroducir «*durante un período limitado controles fronterizos nacionales adaptados a la situación*» de orden público o seguridad nacional. Según el mismo artículo el Estado tiene que consultar previamente a las demás partes firmantes, pero, si «*el orden público o la seguridad nacional exigieran una acción inmediata*», el Estado de que se trate «*adoptará las medidas necesarias e informará de ello lo antes posible a las demás partes*». No hay, de hecho, ningún control sobre los procedimientos de revisión de la exención, la medida puede ser decidida e introducida unilateralmente y, por lo tanto, se excluye de hecho todas las comprobaciones en cuanto a su proporcionalidad y respeto, por parte de las autoridades públicas, de los derechos fundamentales y las libertades individuales[596]. El uso de las excepciones a menudo representa un riesgo real para la preservación de la libre circulación consagrada en el Acuerdo, tanto más al no existir, de hecho, ningún control sobre la proporcionalidad de las medidas adoptadas de esta manera. El recurso de una disposición de los Acuerdos de Schengen debería permitir ejercer un control de proporcionalidad basado en los Tratados y en la jurisprudencia en tanto afecta a las libertades fundamentales, pero en la práctica, tal control no se ejerce.

20. El Acuerdo «*constituyó un hito para la política europea contra el terrorismo*»[597], aunque el primer objetivo que persigue la eliminación de las fronteras entre los Estados miembros de la UE ha sido, sin duda, la realización de la libertad de circulación y el mercado único. La ausencia de fronteras interiores en el Espacio Schengen «*exige una gestión sólida*

[595] La cooperación Schengen se integró en el Derecho de la Unión Europea por el Tratado de Ámsterdam en 1997. Manuel HEREDERO HIGUERAS (2006), «La protección de los datos de interés policial y judicial en la Unión Europea. De Schengen a Prüm», en *Revista Jurídica de Navarra*, núm. 42, págs. 120 y ss.

[596] Este criterio de proporcionalidad en su lugar debería estar asegurado desde que el Acuerdo de Schengen entró, con el Tratado de Amsterdam, a formar parte del Derecho comunitario, y por lo tanto respetar los principios. Ampliamente véase el análisis del artículo 2, apartado 2, en Joanna APAP and Sergio CARRERA (2003), «Maintaining Security within Borders: Towards a Permanent State of Emergency in the EU?», en *CEPS Policy Brief - Centre for European Policy Studies*, núm. 41, págs. 13. Disponible en Internet: https://www.ceps.eu/publications/maintaining-security-within-borders-towards-permanent-state-emergency-eu [consulta: 11 de febrero de 2016]. En este propósito, el escrito destaca, entre otros, dos episodios como ejemplos del uso de los Estados miembros al artículo 2, apartado 2. El primero adoptado por Italia para evitar disturbios durante el G8 de 2001 en Génova, en el que, en esta ocasión, fueron bloqueados en la frontera un importante grupo de personas, y no por el procedimiento "*case-by-case*" previsto por el *acquis* de Schengen. Otro caso se refiere a las autoridades nacionales españolas que han utilizado la cláusula de excepción más que cualquier otro Estado Schengen (hasta el 2003). Medidas de control de las fronteras se volvieron a introducir no sólo durante la Presidencia española de la UE (en las reuniones del Consejo de Sevilla y Barcelona de 2002), sino también en situaciones en que las razones de emergencia no estaban tan claras con el fin "excepcional" para aplicar el artículo 2, apartado 2 (págs. 4 y 5).

[597] Cristina BLASI CASAGRAN (2015: 129).

y fiable de la circulación de personas en las fronteras exteriores». Esta es una circunstancia preliminar para «*garantizar un alto nivel de seguridad interior y la libre circulación de personas*» dentro de este Espacio. Conjuntamente, «*la ausencia de fronteras interiores significa que las autoridades policiales de los Estados miembros también tienen acceso a los datos de las personas*» que circulan[598].

21. Pero es innegable que la eliminación de las fronteras también ha favorecido la posibilidad para que los criminales se muevan más libremente y ha facilitado el desarrollo de sus actividades ilegales. Esto ha puesto en riesgo la seguridad interna de los Estados miembros, que, por mucho tiempo no han reconocido formalmente la necesidad de que se desarrolle una acción positiva desde la Unión. Eso, sin duda, cambió cuando los Estados se percataron de la imposibilidad de llevar a cabo la lucha contra el terrorismo y otras graves forma de delincuencia como una prerrogativa exclusiva de los Estados, dada la naturaleza transnacional del problema que las respuestas nacionales eran incapaces de resolver[599]. Es en ese momento cuando el control de «*las fronteras externas de los Estados miembros y, concretamente, a los nacionales de terceros Estados que entraban en territorio europeo*»[600], pasa a ser el objetivo principal del Acuerdo, como evidente necesidad de una respuesta unificada contra cualquier amenaza a la seguridad nacional.

22. El Acuerdo persigue controlar, en el espacio común, el «*cruce de fronteras interiores*» y «*exteriores*», las peticiones de «*asilo*» y la «*cooperación policial*» y «*judicial*» penal con la finalidad de otorgar mayor seguridad[601]. Para hacer efectivo aquel objetivo se adoptan ciertas medidas, entre las que aquí interesa la creación del Sistema de Información Schengen (en adelante, SIS I y SIS II), que fue uno de sus ejes fundamentales, creado y

[598] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final. Sobre este asunto, véanse Rosario SERRA CRISTÓBAL (2018), «El control de datos de circulación de personas en la UE como mecanismo de salvaguarda de la seguridad nacional», en *UNED. Revista de Derecho Político*, N. 102, mayo-agosto 2018, págs 305-332.

[599] «*La construcción europea, centrada en el desarrollo económico, fue incapaz durante ese período de incrementar un desarrollo armónico y progresivo entre el espacio de libertad, entendido éste como el ámbito de desarrollo de las libertades de circulación de personas, mercancías, capitales y servicios, y el espacio de seguridad* (…) *y ello porque la simple cooperación entre Estados miembros, en lugar del trabajo conjunto en todo el territorio de la Comunidad ofrecía serios inconvenientes, pues se carecía de una estructura integrada de alcance propiamente comunitario*». José Carlos FERNÁNDEZ ROZAS (2004), «El Espacio de Libertad, Seguridad y Justicia consolidado por la Constitución Europea», en *Revista Juridica Española La Ley*, 4, D-195, págs. 2 y ss.

[600] Cristina BLASI CASAGRAN (2015: 129).

[601] *Vid*. ACERVO DE SCHENGEN - CONVENIO DE APLICACIÓN DEL ACUERDO DE SCHENGEN.

regulado en el Título IV (Sistema de Información de Schengen)[602], y el Sistema de Información de Visados (VIS).

23. Los artículos 92 a 119 del CAAS (Título IV) trataban sobre el SIS I o de primera generación[603], un sistema compuesto por secciones nacionales de cada Estado miembro que permite transferir a las autoridades competentes de los Estados miembros, «*de una manera rápida y efectiva, toda la información sobre controles de fronteras y desplazamiento*»[604] de algunas categorías de personas y objetos. Esta información es compartida entre los Estados participantes que firmaron el Acuerdo de Schengen[605].

24. El SIS I representa, todavía hoy en día, la medida más importante de intercambio directo de información en el ámbito de la Unión sobre las personas puestos bajo vigilancia para la prevención y represión[606]. Se trata de «*un sistema centralizado, utilizado por 25 Estados miembros de la UE*» (todos excepto Chipre, Irlanda y Croacia) y cuatro países asociados a Schengen[607], «*que contiene en la actualidad 63 millones de descripciones*»[608]. La base de datos SIS[609] está en Estrasburgo y a ella tienen acceso todos los Estados parte y, sin embargo, cada Estado es responsable de la información aportada.

[602] Capítulo I (Creación del Sistema de Información de Schengen), en ACERVO DE SCHENGEN - CONVENIO DE APLICACIÓN DEL ACUERDO DE SCHENGEN de 14 de junio de 1985.
[603] «Sistema de Información Schengen de segunda generación (SIS II)», en *Agencia Española de Protección de Datos*.
[604] Cristina BLASI CASAGRAN (2015: 129).
[605] El Espacio Schengen se ha extendido poco a poco a casi todos los Estados miembros. Italia firmó los acuerdos el 27 de noviembre de 1990; España y Portugal, el 25 de junio de 1991; Grecia, el 6 de noviembre de 1992; Austria, el 28 de abril de 1995, y Dinamarca, Finlandia y Suecia, el 19 de diciembre de 1996. La República Checa, Estonia, Letonia, Lituania, Hungría, Malta, Polonia, Eslovenia y Eslovaquia se sumaron el 21 de diciembre de 2007, y el País asociado Suiza lo hizo el 12 de diciembre de 2008. El Reino Unido e Irlanda se adhieren sólo parcialmente, mediante el aprovechamiento de la cláusula de salida ("*opt-out*"), mientras que Bulgaria, Rumania, Croacia y Chipre aún tienen que aplicar en su totalidad.
[606] El artículo 93 del CAAS definía el objeto del SIS en términos de «*preservar el orden y la seguridad públicos, incluida la seguridad del Estado, y la aplicación de las disposiciones del presente Convenio sobre la circulación de personas por los territorios de las Partes contratantes, con la ayuda de la información transmitida por dicho sistema*», delimitándose en el artículo 94 las categorías de datos susceptibles de intercambio y añadiéndose una cláusula de salvaguardia de la privacidad por remisión específica al «*artículo 6 del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas en lo referente al tratamiento informatizado de datos de carácter personal*» y a las demás «*obligaciones internacionales*» que afecten a las Partes contratantes. Beatriz S. TOMÁS MALLÉN (2014: 218).
[607] Suiza, Liechtenstein, Noruega e Islandia.
[608] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.
[609] El SIS actualmente contiene alrededor de 70 millones de entradas y fue consultado 2900 millones de veces en 2015, 1000 millones de veces más que en 2014. *Vid*. «Refuerzo del Sistema de Información de Schengen para mejorar la lucha contra el terrorismo y la delincuencia transfronteriza», en *Diario La Ley*, Wolters Kluwer, 20-1-2017.

25. A través de los años se ha producido una evolución de la naturaleza y funciones del SIS hasta un sistema de segunda generación, llamado SIS II, que ha previsto una ampliación de las características de los datos, un aumento de las categorías, así como la especificidad de la información, y «*que incorporara los últimos avances tecnológicos en el campo de la información*»[610]. Esta expansión en cuanto "sistema de intercambio de información entre los Estados" se produjo después de los ataques terroristas del 11 de septiembre de 2001 y otros en Madrid y Londres, que motivaron el desarrollo de una política de seguridad que propició una evolución del SIS, desde su condición de instrumento sencillo para el control de fronteras[611], hasta convertirse en "un sofisticado sistema de información e investigación" diseñado con la finalidad de fortalecer el procedimiento de "intercambio de información en la lucha contra el terrorismo", incluyendo la posibilidad de que Europol tenga acceso a los datos del mismo[612].

26. En este sentido, en los años 2006 y 2007, se aprueban el nuevo Reglamento y Decisión sobre el establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II). El SIS II se rige por el Reglamento (CE) n. 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (en adelante, Reglamento SIS II), que constituye «*la base jurídica que regula el sistema en lo que respecta a los procedimientos de descripción previstos en el Título IV del Tratado constitutivo de la Comunidad Europea (antiguo primer pilar)*»[613]; o

[610] Cristina BLASI CASAGRAN (2015: 130). Ben HAYES (2004), «Statewatch analysis. From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained», en *Statewatch Report*, London, págs. 17 y ss. Disponible en Internet: http://www.statewatch.org/news/2005/may/analysis-sisII.pdf [consulta: 21 de febrero de 2016].

[611] El sistema SIS se presentaba como una base de datos técnicamente no complejo, creado para tratar principalmente información analógica. Además, su estructura no permitió su empleo en un número excesivo de Estados.

[612] REGLAMENTO (CE) N. 871/2004 DEL CONSEJO, de 29 de abril de 2004, relativo a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo, *Diario Oficial de la Unión Europea*, L 162 de 30/04/2004, págs. 0029 – 0031. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0871 [consulta: 01 de marzo de 2016]; DECISIÓN 2005/211/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo, *Diario Oficial de la Unión Europea*, L 68 de 15.3.2005. Disponible en Internet: https://www.unodc.org/tldb/pdf/2005-211-JAI_ES.pdf [consulta: 01 de marzo de 2016].

[613] REGLAMENTO (CE) N. 1987/2006 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 20 de diciembre de 2006 relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), *Diario Oficial de la Unión Europea*, L 381 de 28.12.2006, págs. 4–23. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006R1987 [consulta: 07 de marzo de 2016]. «*El Reglamento sobre el SIS II determina los aspectos técnicos y el método de funcionamiento del SIS II, las modalidades de descripción de nacionales de terceros países a efectos de denegación de entrada o de estancia, y el tratamiento de los datos relativos a descripciones, así como las condiciones de acceso a los datos y su protección*». *Vid*. «Sistema de información Schengen de segunda

bien por la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (en adelante, Decisión SIS II) «*relativa a los procedimientos recogidos en el Título IV del Tratado de la Unión Europea (antiguo tercer pilar)*»[614]. Ambos contienen «*varios artículos comunes que se completan con un conjunto de disposiciones específicas que rigen el uso del sistema en el ámbito concreto de cada uno de los instrumentos*»[615].

27. La versión más reciente del Sistema de Información de Schengen (SIS II), entró en funcionamiento el 9 de abril de 2013 como resultado de una nueva Decisión SIS II[616], que sustituye parte de la normativa del SIS I[617] y se distingue principalmente por la inclusión en las bases de datos nacionales de fotos, huellas digitales y, en especial, los datos biométricos. También, como se ha indicado, Europol[618] y Eurojust tienen acceso al SIS II. Europol ha comenzado a trabajar en un uso más intensivo de las bases de datos, a través de la aplicación de las conclusiones del Consejo JAI de 20 de noviembre de 2015 (en materia de lucha antiterrorista) con el fin de «*comprobar sistemáticamente las bases de datos de Europol y el*

generación (SIS II) - reglamento del antiguo primer pilar», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14544#KEYTERMS [consulta: 13 de marzo de 2016].

614 DECISIÓN 2007/533/JAI DEL CONSEJO, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), *Diario Oficial de la Unión Europea*, L 205 de 7.8.2007, págs. 63–84. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32007D0533 [consulta: 13 de marzo de 2016]. «*La Decisión incluye disposiciones sobre los aspectos técnicos y el funcionamiento del SIS II, las responsabilidades de la autoridad de gestión y de los países participantes, el procesamiento de datos referentes a las descripciones que contendrá el sistema y las condiciones de acceso y protección de los datos. Más concretamente, define las descripciones de personas y bienes que se introducirán en el SIS II al objeto de facilitar la cooperación policial y judicial en materia penal. También incluye disposiciones sobre las condiciones y procedimientos para emitir estas descripciones, y sobre las autoridades que tendrán derecho de acceso a esta información. Concretamente, la Decisión define las categorías de datos (descripciones de personas y bienes) que se introducirán en el sistema como apoyo de la cooperación operativa entre autoridades policiales y entre autoridades judiciales en materia penal, los fines para los que se introducirán, los criterios de introducción y tratamiento, y las autoridades con derecho de acceso a ellos*». «Sistema de información Schengen de segunda generación (SIS II) - reglamento del antiguo primer pilar», en *EUR-Lex*; «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*.

615 «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14569 [consulta: 29 de marzo de 2016].

616 DECISIÓN DEL CONSEJO DE 7 DE MARZO DE 2013, por la que se fija la fecha de aplicación de la Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (2013/157/UE), *Diario Oficial de la Unión Europea*, L 87 de 27.03.2013, págs. 8-9. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013D0157 [consulta: 15 de marzo de 2016].

617 Con la entrada en vigor del marco legal del Sistema de Información Schengen de segunda generación (SIS II), el 9 de abril de 2013, los artículos 92 a 119 del CAAS (Título IV) fueron sustituidos por la normativa incluida en el referido marco legal.

618 El acceso de Europol al SIS II ha sido encaminado el 10 de diciembre de 2014 (*vid*. *infra*).

SIS II»[619], introduciendo búsquedas por lotes en el SIS[620]. No obstante, estos dos organismos sólo tienen acceso «*a la información específica que necesiten para la ejecución de sus misiones*»[621].

28. La nueva regulación del SIS aumenta sus funciones con el fin de acentuar su naturaleza como instrumento de investigación a través de la ampliación del ámbito objetivo de la información contenida en las bases de datos que incluyen «*datos biométricos, como las huellas dactilares y fotografías, de personas con una orden de busca y captura, personas desaparecidas, personas con un procedimiento judicial abierto o bien que están sometidas a vigilancia discreta*»[622]. El SIS II constituye «*un sistema de información a gran escala*» con descripciones de personas y bienes"[623]. Esta información es introducida y consultada por las autoridades competentes, como las fuerzas y cuerpos de seguridad policía y los

[619] CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015d), Conclusiones del Consejo de la UE y de los Estados miembros reunidos en el Consejo en materia de lucha antiterrorista, 20.11.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/11/20-jha-conclusions-counter-terrorism/ [consulta: 15 de marzo de 2016].

[620] Europol ha revisado su plan de trabajo para 2016 con el fin de mejorar el acceso a las grandes bases de datos, entre las que se incluyen el SIS II, el VIS y el sistema Eurodac, y de abordar las cuestiones relativas a la interoperabilidad de los sistemas. Actualmente Europol efectúa comprobaciones manuales en el SIS II y el uso del sistema es bastante reducido (en 2015, el primer año en que Europol tuvo acceso al sistema, se hicieron tan solo 741 búsquedas). INFORME sobre la aplicación de la declaración de los miembros del Consejo Europeo de 12 de febrero de 2015, de las Conclusiones del Consejo JAI de 20 de noviembre de 2015 y de las Conclusiones del Consejo Europeo de 18 de diciembre de 2015, 6785/16, Bruselas, 4 de marzo de 2016, pág. 14. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/es/pdf [consulta: 16 de marzo de 2016].

[621] «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*.

[622] Cristina BLASI CASAGRAN (2015: 130).

[623] «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*. DECISIÓN 2007/533/JAI DEL CONSEJO, de 12 de junio de 2007. Los datos introducidos en el SIS I fueron el nombre y apellido de la persona, alguna característica física, lugar y fecha de nacimiento, sexo y nacionalidad, o si la persona estaba armada o se considera peligrosa. Así como había sido originalmente previsto, el SIS alojaba principalmente información de caracteres alfanuméricos. A tales datos pudieron acceder, dentro de los límites de sus áreas de competencia, las autoridades de policía, las autoridades de control de fronteras, las aduanas y las autoridades judiciales en el proceso penal. El SIS II es «*una base de datos sofisticada que permite a las autoridades responsables de los Estados de Schengen intercambiar datos sobre determinadas categorías de personas y bienes*» (se puede informar de vehículos, armas de fuego, documentos de identidad y cheques bancarios desaparecidos o robados). «El espacio y la cooperación Schengen», en *EUR-Lex*. El sistema SIS II almacena datos sobre las personas descritas, incorporando nuevas funcionalidades: «*nombres y apellidos, nombres y apellidos de nacimiento, nombres y apellidos anteriores y alias*», «*rasgos físicos particulares*», «*lugar y fecha de nacimiento*», «*sexo*», «*fotografías*», «*impresiones dactilares*», «*nacionalidad o nacionalidades*», «*indicación de que las personas en cuestión están armadas, son violentas o se han escapado*», «*motivo de la inscripción*», «*autoridad informadora*», «*una referencia a la decisión que haya dado lugar a la descripción*», y «*la conexión o conexiones con otras descripciones introducidas en el SIS II*». Se incluirá también la conducta que deba observarse en caso de una respuesta positiva (es decir, si una autoridad nacional competente encuentra en el SIS II una descripción de un nacional de un país tercero al que está investigando). Si el Estado miembro no pudiera ejecutar la acción pertinente tras obtener una respuesta positiva, informará de ello inmediatamente al Estado miembro que haya introducido la descripción. En particular, *vid*. artículo 20 (Categorías de datos); artículo 26 (Objetivos y condiciones de las descripciones), artículo 32 (Objetivos y condiciones de las descripciones), artículo 34 (Objetivos y condiciones de las descripciones), artículo 36 (Objetivos y condiciones de las descripciones) y artículo 38 (Objetivos y condiciones de las descripciones) de la Decisión SIS II.

servicios de control fronterizo, inmigración, «*las autoridades encargadas de velar por el cumplimiento de la ley*», y pueden utilizarlas con el «*objeto de garantizar un alto nivel de seguridad*»[624]. Siguiendo esa línea, el SIS II tiene por finalidad: «*garantizar un alto nivel de seguridad en el espacio de libertad, seguridad y justicia de la Unión Europea, incluidos el mantenimiento de la seguridad pública y del orden público y la salvaguardia de la seguridad en el territorio de los Estados miembros, y aplicar las disposiciones del título IV de la Tercera parte del Tratado CE relativas a la circulación de personas en dicho territorio, con la ayuda de la información transmitida por este sistema*»[625].

29. Ambas normas, Decisión y Reglamento, contienen reglas sobre protección de datos bastante similares. No obstante, solo la Decisión SIS II hace mención al Convenio n. 108: «*Los datos personales que se traten en aplicación de la presente Decisión se protegerán de conformidad con el Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, y sus modificaciones posteriores*»[626]. Esto significa que cuando el uso de los datos personales por parte de las autoridades nacionales de policía se lleva a cabo de conformidad con la Decisión del SIS II, las disposiciones del Convenio n. 108 y de la Recomendación R (87) 15 del Comité de Ministros a los Estados miembros «*dirigida a regular la utilización de datos de carácter personal en el sector de la policía*», deberán aplicarse en la legislación nacional[627]. El Convenio también «*se tomará como referencia para definir las categorías de datos cuyo tratamiento en el SIS II estará prohibido*»[628].

30. A través del SIS, operativo desde 1995, «*los Estados miembros pueden mandar una descripción ("alert") de personas que estén en busca y captura, o vinculadas a investigaciones policiales o a procedimientos penales, o también a las que se le haya denegado el acceso al Espacio Schengen*»[629]. Será introducido «*una descripción cuando la*

[624] «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*.
[625] Artículo 1 (Establecimiento y finalidad general del SIS II) de la Decisión SIS II y del Reglamento SIS II.
[626] Artículo 57 (Aplicación del Convenio del Consejo de Europa sobre protección de datos) de la Decisión SIS II.
[627] Considerandos 19 y 20 de la Decisión SIS II.
[628] «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*.
[629] Cristina BLASI CASAGRAN (2015: 129). «*Las búsquedas por vía del SIS pueden emitir una respuesta («hit/no hit»), que especifica la acción a seguir contra personas a las que se le veta la entrada al Espacio Schengen*». Faustoluigi MEROLA (2016), «Decisione di Esecuzione (UE) 2016/1209 della Commissione del 12/07/2016. Disposizioni di attuazione per il sistema d'informazione Schengen di seconda generazione (SIS II)», en *AmbienteDiritto.it*, págs. 5 y ss. Disponible en Internet:

decisión (…) *se base en la amenaza que para el orden público o la seguridad nacional pueda constituir la presencia de un nacional de un tercer país en el territorio de un Estado miembro*»[630]. La característica específica del SIS en comparación con otros instrumentos de intercambio de información es que «*su información se complementa con una instrucción para que los agentes que trabajan sobre el terreno tomen medidas concretas, como la detención o incautación*»[631].

31. La introducción, actualización, supresión y consulta de datos del SIS II se realiza a través de los distintos sistemas de información nacionales (N.SIS) conectados a un sistema de información central (C.SIS)[632], situado en Estrasburgo, y a «*una infraestructura de comunicación entre el sistema central y los sistemas nacionales*»[633]. El sistema central contiene ciertos datos introducidos por los Estados miembros sobre personas y bienes, y es utilizado por las autoridades nacionales encargadas de controles fronterizos, por la policía, por las autoridades aduaneras, las autoridades competentes para la expedición de visados y las autoridades judiciales en el Espacio Schengen[634]. Cada Estado miembro es responsable de la creación, la puesta en funcionamiento y el mantenimiento de su propio sistema nacional

https://www.ambientediritto.it/home/dottrina/decisione-di-esecuzione-ue-20161209-della-commissione-del-12072016 [consulta: 16 de agosto de 2017].

630 «*Los datos relativos a los nacionales de terceros países para los que se haya introducido una descripción a efectos de denegación de entrada o estancia se introducirán sobre la base de una descripción nacional resultante de una decisión adoptada, observando las normas de procedimiento previstas por la legislación nacional, por las autoridades administrativas o por los órganos jurisdiccionales competentes. Esta decisión sólo podrá tomarse sobre la base de una evaluación del caso concreto*». Artículo 24 (Condiciones para introducir descripciones a efectos de denegación de entrada o de estancia) del Reglamento SIS II.

631 COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

632 Artículo 4 (Arquitectura técnica y funcionamiento del SIS II) del Reglamento SIS II. «*La gestión operativa del SIS II Central consistirá en todas las funciones necesarias para mantenerlo en funcionamiento durante las 24 horas del día, 7 días a la semana*», de conformidad con el Reglamento (CE) n. 1987/2006 del Parlamento Europeo y del Consejo. Artículo 15 (Gestión operativa) del Reglamento SIS II.

633 «Sistema de información Schengen de segunda generación (SIS II) - reglamento del antiguo primer pilar», en *EU-Lex*.

634 Cada Estado miembro administra una copia nacional del C.SIS, conocido como el Sistema de Información Nacional de Schengen (N.SIS), que se actualiza constantemente, actualizando así el sistema central. El sistema nacional es consultado y se proporciona a la señal en al menos uno de los siguientes casos: la persona no tiene derecho a entrar o permanecer en el territorio de las Schengen; la persona o bien es buscados por las autoridades judiciales o las autoridades policiales; se ha denunciado a la persona como desaparecida; o los bienes tales como billetes de banco, automóviles, vehículos comerciales, armas y documentos de identidad han sido robados o perdidos. En esos casos, deberán iniciarse actividades de seguimiento a través de los Sistemas Nacionales de Información Schengen. Artículo 4 (Arquitectura técnica y funcionamiento del SIS II) y Artículo 38 (Objetivos y condiciones de las descripciones) de la Decisión SIS II.

y de la conexión de éste al sistema central[635]. Este sistema de TI de Schengen[636] (N.SIS y C.SIS) se completa por una red virtual cifrada dedicada a los datos del SIS II denominada *SIRENE* ("*Supplementary Information Request at the National Entry*")[637], una «*infraestructura de comunicación entre el sistema central y los sistemas nacionales*» que prevé «*el intercambio de información entre las autoridades*» responsables del intercambio de toda la información complementaria[638]. Esta red es, por lo tanto, una de las principales herramientas que se utilizan para asegurar las diversas políticas que subyacen a la realización del ELSJ, por medio de intercambio de datos e información entre las autoridades europeas y nacionales competentes[639].

32. Los datos tratados en el SIS II no se transfieren a países fuera de la UE –que no formen parte del Acuerdo– ni a organizaciones internacionales, ni se ponen a su disposición[640].

33. Si son conservados datos sobre una persona, el interesado tiene derecho a solicitar el acceso a los datos para averiguar la corrección y la legitimidad de estos o a hacer suprimir los que se hayan almacenado de manera ilegal[641]. Si no existen tales condiciones, el sujeto

[635] Cada Estado miembro designará igualmente una autoridad, la oficina SIS II nacional, que asumirá la responsabilidad central respecto de su proyecto SIS II nacional. Dicha autoridad será responsable del correcto funcionamiento y la seguridad de su sistema nacional. Artículo 7 (Oficina N. SIS II y Servicio Nacional *SIRENE*) del Reglamento SIS II.

[636] CONSEJO DE LA UNIÓN EUROPEA (2009), 2009 Catálogo de Schengen. Recomendaciones y prácticas más idóneas SIS, 16613/3/08, REV 3, Bruselas, 8 de mayo de 2009 (29.05), pág. 21. Disponible en Internet: http://www.intermigra.info/archivos/impresos/CatScheng.pdf [consulta: 21 de marzo de 2016].

[637] «Sistema de información Schengen de segunda generación (SIS II) - reglamento del antiguo primer pilar», en *EU-Lex*. Raquel CASTILLEJO MANZANARES (2013: 294-295).

[638] «Sistema de información Schengen de segunda generación (SIS II) - reglamento del antiguo primer pilar», en *EU-Lex*. Federico DECLI, Gabriella MARANDO (2009: 107); Joanna PARKIN (2011a), «The Schengen Information System and the EU Rule of Law», en *INEX Policy Brief Centre for European Policy Studies (CEPS)*, núm. 13, págs. 9. Disponible en Internet: https://www.ceps.eu/publications/schengen-information-system-and-eu-rule-law [consulta: 13 de marzo de 2016].

[639] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final. «*Las comprobaciones en el SIS son obligatorias a efectos de la tramitación de visados para estancias de corta duración, para el control fronterizo de nacionales de terceros países y, de forma no sistemática, para los ciudadanos de la UE y otras personas que disfrutan del derecho a la libre circulación. Además, cada control policial en el territorio debe incluir un control automático en el SIS*».

[640] Considerando 14 y artículo 39 (Transferencia de datos personales a terceras partes) del Reglamento SIS II.

[641] Artículo 58 de la Decisión SIS II y; artículo 59 de la Decisión SIS II Tanto para la Decisión SIS II como para el Reglamento SIS II, los derechos de acceso de las personas en relación con el SIS II pueden ejercerse en cualquier Estado miembro y se tratarán de conformidad con la legislación nacional de ese Estado miembro. Por lo que se refiere al «*derecho de rectificación y supresión*», «*se informará a la persona interesada lo antes posible del resultado del ejercicio de sus derechos* (…) *y, en todo caso, en el plazo máximo de tres meses desde la fecha en que solicitó la rectificación o la supresión*». En resumen, toda persona podrá emprender acciones ante los órganos jurisdiccionales o las autoridades competentes para «*acceder, rectificar, suprimir u obtener información o una indemnización en relación con una descripción que se refiera a ella*», remitiéndose además al control ejercido por la autoridad o autoridades designadas en cada Estado miembro y al llevado a cabo por el SEPD. Artículo 41 (Derecho de acceso, rectificación de datos que contengan errores y supresión de datos

tiene derecho a solicitar la corrección o eliminación. En general, las descripciones relativas a personas y bienes sólo pueden conservarse en el SIS II «*durante el tiempo necesario para alcanzar los fines para los que hayan sido introducidas*». De conformidad con la Decisión y el Reglamento, «*los Estados miembros deberán examinar la necesidad de mantener una descripción de una persona en un plazo de tres años tras su introducción en el SIS II*». La Decisión SIS II incorpora «*garantías adicionales con la reducción de este período a un año en el caso de las descripciones de personas para controles discretos o específicos. Los Estados miembros pueden acortar estos plazos de revisión de conformidad con su legislación nacional*»[642]. Además, las normas prohíben el tratamiento de datos sensibles[643]. Según el Reglamento SIS II, no se permite el tratamiento de categorías de datos sensibles, según lo mencionado en el artículo 9, apartado 1, del RGPD.

34. El acceso puede ser denegado sólo «*cuando sea indispensable para la ejecución de una medida legal consignada en la descripción*», así como para proteger «*los derechos y libertades de otras personas*»[644]. No se proporcionará el derecho a ser informado[645], si 1) los datos personales no han sido obtenidos del interesado y si dicha información es imposible o requiere un esfuerzo desproporcionado, 2) el interesado ya tenga la información o 3) si el Derecho nacional permita una restricción basada, entre otras cosas, en la protección de la seguridad nacional, la defensa, la seguridad pública o la prevención de delitos penales.

35. La autoridad o autoridades nacional de control competentes de cada Estado miembro, investidas de los poderes a los que se refiere el RGPD[646], son las encargadas de controlar, con total «*independencia*», «*la legalidad del tratamiento de los datos personales del SIS II dentro de su territorio*» e «*incluido el intercambio y posterior tratamiento de la información*

que se hayan almacenado de manera ilegal) del Reglamento SIS II y artículo 43 (Recursos) del Reglamento SIS II. *Vid*. Beatriz S. TOMÁS MALLÉN (2014: 238). Cada Estado miembro será responsable «*de cualquier daño ocasionado a una persona como consecuencia de la utilización de su sistema nacional N.SIS II*». Artículo 64 (Responsabilidad) de la Decisión SIS II. Los Estados miembros garantizarán que cualquier posible «*utilización incorrecta de los datos del SIS II y todo intercambio de información complementaria contrario a lo dispuesto en el presente Reglamento estén sujetos a sanciones eficaces, proporcionadas y disuasorias* (…)». Artículo 49 (Sanciones) del Reglamento SIS II.

642 «Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*. La Decisión SIS II contiene disposiciones específicas sobre los períodos máximos de conservación de las descripciones de bienes (5 o 10 años en función del tipo de descripción).

643 Artículo 56 de la Decisión SIS II y artículo 40 del Reglamento SIS II (Tratamiento de las categorías sensibles de datos).

644 Artículo 58 (Derecho de acceso, rectificación de datos que contengan errores y supresión de datos que se hayan almacenado de manera ilegal) de la Decisión SIS II.

645 Artículo 42 (Derecho de información), apartado 2, del Reglamento SIS II.

646 Capítulo VI - Autoridades de control independientes, del RGPD. Antes se hacía referencia al artículo 28 (Autoridad de control) de la Directiva 95/46/CE.

complementaria»[647]. En particular, «*deberá comprobar la calidad de los datos que el Estado miembro introduce en el sistema*» central a través del sistema nacional[648]. La autoridad nacional de supervisión «*velará por que, al menos cada cuatro años, se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los N.SIS II*» nacionales[649]. El SEPD se encarga de controlar que «*las actividades de tratamiento de datos personales de la Autoridad de Gestión sean conformes*» al Reglamento y Decisión[650]. Las autoridades nacionales de control y el SEPD cooperan y garantizan una supervisión coordinada de la Decisión del SIS II[651], mientras que el SEPD es responsable de la supervisión del sistema central (C.SIS)[652].

36. El nuevo sistema de información plantea algunos problemas acerca de la protección de los datos personales de aquellos que se encuentran sujetos a sus controles y, en particular, sobre sus instrumentos de protección[653]. Aspectos problemáticos emergen con especial atención con respecto a la utilización de datos biométricos (por ejemplo: ADN, huellas dactilares, escaneo del iris), como una herramienta en la identificación de los sujetos y sus posibles resultados erróneos. En efecto, la información biométrica se incluye, de hecho, entre los datos puestos a disposición, aunque la Decisión SIS II no especifica las características de estos últimos, sin embargo, previendo un estudio preventivo de la Comisión en la materia y dejando la elección final a las autoridades nacionales competentes[654]. Por otra parte, un problema adicional se deriva de que el Convenio de Schengen no prevé ninguna referencia a la protección de la privacidad, así que la protección de los ciudadanos se deja a las normas previstas por los sistemas jurídicos nacionales. A éste se añade el problema adicional de los

[647] Artículo 44 (Supervisión de las N. SIS II) del Reglamento SIS II.
[648] Artículo 60 (Supervisión de las N.SIS II) de la Decisión SIS II y artículo 44 del Reglamento SIS II.
[649] Artículo 60 (Supervisión de las N.SIS II) de la Decisión SIS II y artículo 44 del Reglamento SIS II.
[650] Artículo 61 (Supervisión de la Autoridad de Gestión) de la Decisión SIS II y artículo 45 del Reglamento SIS II.
[651] Las autoridades nacionales de control y el SEPD deben cooperar activamente en el marco de sus responsabilidades y garantizar una supervisión coordinada del SIS II: «*intercambiarán la información pertinente, se asistirán mutuamente en la realización de auditorías e inspecciones*», delineando «*propuestas armonizadas*» para soluciones comunes a problemas potenciales y promoviendo el conocimiento de los derechos de protección de datos. Las autoridades nacionales de control y el SEPD se reunirán al menos dos veces al año. *Vid*. artículo 62 (Cooperación entre las autoridades nacionales de control y el Supervisor Europeo de Protección de Datos) de la Decisión SIS II y artículo 46 del Reglamento SIS II.
[652] Con el fin de garantizar la transparencia, se debe remitir al Parlamento Europeo, al Consejo, a la Comisión y a la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (*eu-LISA*) un informe conjunto sobre las actividades realizadas. Artículo 62, apartado 3, de la Decisión SIS II.
[653] *Amplius*, *vid*. Joanna PARKIN (2011b), «The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law», en *CEPS Paper in Liberty and Security in Europe*, págs. 39. Disponible en Internet: http://aei.pitt.edu/31282/1/SIS_II_paper_liberty_security_formatted1[1].pdf [consulta: 14 de marzo de 2016].
[654] Artículo 22 (Normas específicas para las fotografías y las impresiones dactilares) de la Decisión SIS II.

diferentes grados de protección proporcionados por cada legislación nacional, con el resultado paradójico de que, frente a los sistemas de información del Espacio Schengen puede existir ciudadanos más o menos protegidos[655].

37. De lo anterior se añade entonces una consideración acerca de la incorporación del acervo de Schengen en el marco jurídico de la Unión. Aunque idealmente éste ha reconducido todos los elementos de tutela de los derechos y la legitimidad democrática de la Unión, sin embargo, la forma en que es concebida dicha incorporación ha dado lugar a determinadas debilidades en este sentido. Éstas surgen por la participación diferenciada de los Estados al acervo de Schengen[656].

38. En 2016, la Comisión Europea llevó a cabo una evaluación del SIS[657] que permitió constatar que se habían establecido mecanismos nacionales para permitir que los interesados accedan, rectifiquen y eliminen sus datos personales en el SIS II o para obtener una compensación en relación con datos inexactos. Para mejorar la eficiencia y la eficacia del SIS II, y con ello "mejorar los sistemas de información existentes a fin de promover la seguridad de nuestras fronteras y los derechos individuales", la Comisión Europea presentó tres propuestas de reglamentación[658]. En particular, los cambios propuestos por la Comisión,

---

655 Se vean *supra* los artículos 58 de la Decisión SIS II y 41 del Reglamento SIS II relativos al derecho de acceso, rectificación de datos que contengan errores y supresión de datos que se hayan almacenado de manera ilegal.

656 Sobre el punto, véase la sentencia del Tribunal de Justicia del UE que establece que la cooperación reforzada con arreglo al acervo de Schengen constituye un paralelo al Derecho de la Unión por el hecho de que el número de Estados que participan a menudo se identifica con la totalidad Estados miembros, en TJUE (Gran Sala), *Reino Unido de Gran Bretaña y de Irlanda del Norte contra Consejo de la Unión Europea*, asunto C-482/08, sentencia de 26 de octubre de 2010. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=78737&doclang=ES [consulta: 18 de marzo de 2016].

657 INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre la evaluación del Sistema de Información Schengen de segunda generación (SIS II) de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n. 1987/2006 y el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, COM(2016) 880 final, Bruselas, 21.12.2016.

658 Tal como se anunció en el discurso del Estado de la Unión 2016. Estado de la Unión 2016. El 21 de diciembre de 2016, la Comisión presentó un paquete de medidas legislativas para mejorar la forma en que se utiliza el SIS: PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular, COM(2016) 881 final - 2016/0407(COD), Bruselas, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016PC0881 [consulta: 16 de agosto de 2017]; PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1987/2006, COM(2016) 882 final - 2016/0408(COD), Bruxelles, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52016PC0882R(01) [consulta: 16 de agosto de 2017]; PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n.

permitirán: mejorar la seguridad y accesibilidad del sistema al establecer requisitos uniformes para los agentes que trabajan sobre el terreno acerca de la manera de procesar los datos del SIS de forma segura y de garantizar la continuidad de las actividades para los usuarios finales; reforzar la protección de datos mediante la introducción de salvaguardias adicionales para garantizar que la recogida y el tratamiento de datos y "el acceso a los mismos se limite a lo estrictamente necesario, en el pleno respeto de la legislación y de los derechos fundamentales de la UE, incluido el derecho a una tutela judicial efectiva"[659]

39. Es importante destacar que las propuestas permiten el tratamiento de otras categorías de datos biométricos, además de fotografías y huellas dactilares, que ya forman parte del régimen SIS II actual. Las huellas dactilares faciales, las huellas digitales y los perfiles de ADN también se almacenarán en la base de datos del SIS. Además, aunque el Reglamento SIS II y la Decisión SIS II preveían la posibilidad de buscar huellas dactilares para identificar a una persona, las propuestas hacen que esta búsqueda sea obligatoria si la identidad de la persona no puede determinarse de otra manera. Las imágenes faciales, fotografías y huellas digitales se utilizarán para buscar en el sistema e identificar a las personas, cuando sea técnicamente posible. Las nuevas reglas sobre datos biométricos presentan riesgos particulares para los derechos de las personas[660].

40. Sin embargo, se señala que, como lo demuestran los recientes atentados en Berlín en diciembre de 2016 y, por último, en Barcelona en agosto de 2017, ni la intensificación de controles policiales en zonas fronterizas ni el restablecimiento de controles fronterizos

1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione, COM(2016) 883 final - 2016/0409 (COD), Bruxelles, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016PC0883&from=EN [consulta: 16 de agosto de 2017].

[659] *Vid*. *amplius*, «La Commissione propone di rafforzare il sistema d'informazione Schengen», en *Rappresentanza in Italia della Commissione europea*, 21-12-2016. Disponible en Internet: https://ec.europa.eu/italy/news/20161221_sis_it [consulta: 18 de agosto de 2017]; «Refuerzo del Sistema de Información de Schengen para mejorar la lucha contra el terrorismo y la delincuencia transfronteriza» (2017).

[660] En su dictamen sobre las propuestas de la Comisión, el SEPD destacó que los datos biométricos son muy sensibles y su introducción en una base de datos a gran escala debería basarse en una evaluación basada en la evidencia de la necesidad de incluirlos en el SIS. En otras palabras, el SEPD recomienda llevar a cabo una evaluación de la necesidad de recoger y utilizar dichos datos en el SIS y de la proporcionalidad de su recogida. El SEPD también consideró que es necesario aclarar qué tipo de información se puede incluir en el perfil de ADN. Dado que el perfil de ADN puede incluir información sensible, los perfiles de ADN almacenados en el SIS deberían contener sólo la información mínima estrictamente necesaria para la identificación de las personas y excluir explícitamente información de salud, origen racial y cualquier otra información sensible. *Vid*. RESUMEN DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la nueva base jurídica del Sistema de Información de Schengen (2017/C 200/08), *Diario Oficial de la Unión Europea*, 23.6.2017.

pueden garantizar la plena seguridad en el Espacio Schengen[661]. Por lo tanto, sigue siendo fundamental una cooperación reforzada y eficaz a todos los niveles de los servicios de los Estados miembros responsables de la lucha contra el terrorismo (intercambio de información, cooperación policial y utilización de bases de datos de la UE). A nuestro juicio, reflexionando sobre este sistema de información, se plantea la cuestión de la necesidad y proporcionalidad de las medidas que deberían complementarse con la evaluación del impacto en el derecho a la protección de datos y el derecho a la intimidad. Sería también más apropiado fortalecer la eficiencia operativa y la eficiencia del Sistema de Información SIS II y de cómo adaptarse a las nuevas necesidades, con el fin de colmar las lagunas de información y mejorar el intercambio de información sobre el terrorismo, la delincuencia transfronteriza y la migración irregular, contribuyendo así a un control más estricto de nuestras fronteras exteriores y una unión de seguridad eficaz y sostenible y la cooperación entre los Estados[662], con el fin de evitar futuros y nuevos ataques contra la seguridad y la

[661] Siguiendo esta tendencia de incremento de la seguridad propiciada por Estados europeos dentro el *acquis* Schengen, se aprobó el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen). El Código de Fronteras Schengen contiene disposiciones relativas al «*control fronterizo de las personas*» que cruzan las fronteras "interiores y exteriores" de los Estados miembros de la Unión, y, sobre todo, prevé un mecanismo de «*restablecimiento temporal de los controles en las fronteras interiores*» (en caso de «*amenaza grave para el orden público o la seguridad interior*»). El Reglamento establece en primer lugar las «*normas aplicables al control fronterizo de las personas que cruzen las fronteras exteriores de los Estados miembros*». Si un nacional de un tercer País es titular de un visado, la «*inspección minuciosa*» a la entrada incluirá también «*la comprobación de la identidad del titular del visado y la de la autenticidad del visado, mediante la consulta del Sistema de Información de Visados (VIS)*». El Reglamento (Capítulo II) prevé que los controles en las fronteras interiores se podrán restablecer con «*carácter excepcional*» en el Espacio Schengen durante un período limitado de tiempo, en los casos en que: «*se presente una amenaza grave para el orden público o la seguridad interior de un Estado miembro, este podrá restablecer los controles fronterizos en partes específicas o en la totalidad de sus fronteras interiores* (…) *no podrá superar los seis meses*»; y en "circunstancias excepcionales" que pongan en riesgo el funcionamiento general del Espacio Schengen sin controles en las fronteras interiores como consecuencia de deficiencias graves persistentes en los controles de las fronteras exteriores, y en la «*medida en que dichas circunstancias representen una amenaza grave para el orden público o para la seguridad interior en el Espacio sin controles en las fronteras interiores o en partes del mismo*». En estos casos, el Consejo podrá recomendar, a propuesta de la Comisión, que uno o más Estados de la Unión restablezcan controles fronterizos en todas sus fronteras interiores o en partes concretas de ellas durante un período máximo de dos años. REGLAMENTO (UE) 2016/399 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen), *Diario Oficial de la Unión Europea*, L 77 de 23.3.2016, págs. 1–52. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0399 [consulta: 12 de agosto de 2017]. También el Reglamento especifica que el restablecimiento temporal de controles fronterizos interiores «*como último recurso y como medida orientada a proteger los intereses comunes dentro del espacio sin controles en las fronteras interiores, y cuando todas las demás medidas sean ineficaces para hacer frente de manera efectiva a la amenaza grave constatada*» (ataques o amenazas terroristas, o amenazas relacionadas con la delincuencia organizada). Francia (en 2015 y 2017), Malta (en 2015) y Italia (en 2017) han restablecido los controles en las fronteras interiores. Sobre este asunto, *vid*. *amplius* SERVIZIO STUDI DEL SENATO (2017: 9 y ss.).

[662] En el pasado, la UE ha llevado a cabo en este sentido: la Directiva 2004/82/CE, establece la obligación de las compañías aéreas para recoger y transmitir a las autoridades fronterizas europeas los datos relativos a sus pasajeros. Sin embargo, esta herramienta no es adecuada para la lucha contra el terrorismo: ha sido pensada para la inmigración ilegal y que se refiere a los datos personales de los pasajeros (nombre, nacimiento, nacionalidad, número de pasaporte), útil sólo para identificar a las personas que ya clasificados como sospechosas. En «Obligación por parte de los transportistas aéreos de comunicar los datos sobre los pasajeros»,

libertad individual. Eso no debe alejarnos del objetivo principal que es al mismo tiempo "garantizar que las autoridades policiales, aduaneras y judiciales competentes las autoridades tienen sistemáticamente la información necesaria para el desempeño de sus funciones; y mantener un equilibrio con respecto a los derechos a la privacidad, la protección de datos y otros derechos fundamentales".

41. Destacando la complejidad del panorama existente de los sistemas de información de la UE, se invita al legislador a reflexionar sobre un marco jurídico más completo, coherente y consistente para los sistemas de información a gran escala de la UE relativos a la gestión de fronteras y la ejecución de leyes en pleno cumplimiento de los principios de protección de datos, por ejemplo: "la limitación de la finalidad; seguridad de última generación; proporcionar períodos de conservación de datos; calidad de los datos; protección de datos desde el diseño; trazabilidad; supervisión eficaz y sanciones disuasorias por uso incorrecto".

3. El Sistema de Información de Visados frente a las amenazas a la seguridad

42. El Sistema de Información de Visados (VIS de las ingles *Visa Information System*)[663], establecido por la Decisión 2004/512/CE del Consejo (en adelante, Decisión VIS), de 8 de junio de 2004, es un sistema centralizado de intercambio de datos sobre visados para estancias de corta duración en el Espacio Schengen entre los Estados que forman parte del mismo[664]. Estos Estados comparten un área común de libre circulación sin controles fronterizos internos. Además, tienen una política de visados común que incluye el intercambio de información de los solicitantes de visados.

43. La institución del Sistema de Información de Visados (en adelante, VIS) constituye una de las iniciativas clave de las políticas de la UE para crear un ELSJ sin fronteras

en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=URISERV:l14582 [consulta: 13 de agosto de 2017].

[663] Visa Information System (VIS). Disponible en Internet: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.

[664] DECISIÓN DEL CONSEJO, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE), *Diario Oficial de la Unión Europea*, L 213 de 15.6.2004, págs. 5–7. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32004D0512 [consulta: 08 de abril de 2016]. Además de a todos los Países de la UE –con excepción del Reino Unido, Irlanda y Dinamarca, que no tomaron parte en su adopción–, la aplicación del marco legal aplicable al VIS se extiende a Islandia, Noruega y Suiza.

interiores[665]. A diferencia del SIS II, el VIS se estableció en el marco del antiguo primer pilar de la Unión. No obstante, se adoptó un instrumento VIS del tercer pilar para que los servicios policiales designados pudieran acceder al sistema a fin de efectuar consultas relacionadas con la comisión de determinadas infracciones[666].

44. El VIS opera a través de un sistema centralizado, el Sistema Central de Información de Visados (CS-VIS, *Central Visa Information System*), conectado a una interfaz nacional en cada Estado miembro (NI-VIS), que proporciona la conexión con las autoridades nacionales centrales de los respectivos Estados miembros, mediante una infraestructura de comunicación entre CS-VIS y NI-VIS[667].

45. El funcionamiento del Sistema se rige por el Reglamento (CE) n. 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS)[668], mientras que «*los procedimientos y condiciones para la expedición de visados de tránsito o para estancias previstas en el territorio de los Estados miembros no superiores a tres meses en un período de seis meses*» se rigen por el Reglamento (CE) n. 810/2009 del Parlamento Europeo y del Consejo de 13 de julio de 2009 por el que se establece un Código comunitario sobre visados[669].

46. El VIS "permite a los Estados Schengen el intercambio de datos sobre visados de corta duración a través de un sistema que conecta los consulados de los Estados Schengen ubicados en países no comunitarios con los puntos de paso de las fronteras exteriores de los

---

[665] «*La idea de crear un sistema de información común para la identificación de los visados se remonta al Consejo Europeo de Sevilla de 2002*». *Vid*. CONCLUSIONES de la Presidencia del Consejo Europeo de Sevilla 21 y 22 de junio de 2002, 13463/02, Bruselas, 24 de octubre de 2002 (29.10), pág. 8. Disponible en Internet: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/es/ec/72639.pdf [consulta: 10 de abril de 2016].

[666] Alejandro Luis GACITÚA ESPÓSITO (2014: 243).

[667] *Vid*. artículo 1 de la DECISIÓN DEL CONSEJO, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE); «Creación de un Sistema de Información de Visados (VIS) - primera etapa», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14516 [consulta: 13 de febrero de 2016].

[668] REGLAMENTO (CE) N. 767/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS), *Diario Oficial de la Unión Europea*, L 218 de 13.8.2008, págs. 60–81. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008R0767 [consulta: 13 de febrero de 2016].

[669] REGLAMENTO (CE) N. 810/2009 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados), *Diario Oficial de la Unión Europea*, L 243 de 15.9.2009, págs. 1–58. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32009R0810 [consulta: 15 de febrero de 2016].

Estados Schengen"[670]. El marco básico determinado por el Reglamento (CE) n. 767/2008 (en adelante, Reglamento VIS) establece un margen de acción muy amplio. Tiene en realidad el objetivo principal de «*mejorar la aplicación de la política común de visados, la cooperación consular y las consultas entre las autoridades centrales de visados, facilitando el intercambio de datos entre los Estados miembros sobre las solicitudes y sobre las decisiones relativas a las mismas* (…)»[671]. También entre los objetivos principales del VIS se encuentra el simplificar los procedimientos de solicitud de los visados, impedir la búsqueda de visados de conveniencia[672], mejorar del control en las fronteras exteriores del Espacio Schengen y «*contribuir a la prevención de amenazas contra la seguridad interior de cualquier Estado miembro*»[673].

47. En ciertos casos, las autoridades nacionales y Europol también pueden solicitar el acceso a los datos almacenados en el VIS para la «*prevención, detección e investigación de delitos de terrorismo y otros delitos graves*»[674]. Estas consultas deben llevarse a cabo a través de puntos de acceso centrales de los países participantes y por Europol, garantizando la verificación de las solicitudes y asegurando el cumplimiento de la Decisión 2008/633/JAI del Consejo[675]. Entonces, tras la adopción de la Decisión anterior también las autoridades nacionales de policía identificados específicamente por el Estado pueden acceder a los datos contenidos en el VIS, siempre que haya «*motivos razonables para considerar que la consulta de los datos del VIS puede contribuir sustancialmente a la prevención, detección o*

[670] REGLAMENTO (CE) N. 810/2009. El Sistema de Información de Visados (VIS) comenzó a funcionar el 11 de octubre 2011 y está siendo desplegado por zonas de acuerdo con la planificación establecida por la Comisión Europea. COMISIÓN EUROPEA - Comunicado de prensa (2011), Entrada en funcionamiento de un sistema de visados más eficaz y seguro, Bruselas, 11 de octubre de 2011. Disponible en Internet: http://europa.eu/rapid/press-release_IP-11-1169_es.htm [consulta: 12 de abril de 2016]. Todos los consulados de los Estados Schengen (alrededor de 2000) y todos sus pasos fronterizos exteriores (unos 1800 en total) se han conectado al sistema. «*En los pasos fronterizos o en el territorio de los Estados miembros, el VIS se utiliza para verificar la identidad de los titulares de visados, comparando sus impresiones dactilares con las impresiones dactilares almacenadas en dicho sistema. Este procedimiento garantiza que la persona que solicitó el visado es la misma que cruza la frontera. Una búsqueda de impresiones dactilares en el VIS también permite identificar a una persona que haya solicitado un visado en los últimos cinco años y que pueda no llevar documentos de identidad*». COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[671] Artículo 2 (Objetivo) del Reglamento VIS.

[672] El Sistema VIS además está dirigido a la prevención del "*visa shopping*" y ayudar a los Estados miembros en la lucha contra el fraude.

[673] Artículo 2 (Objetivo), letra g), del Reglamento VIS.

[674] Artículo 3 (Disponibilidad de los datos para la prevención, detección e investigación de delitos de terrorismo y otros delitos graves) del Reglamento VIS.

[675] DECISIÓN 2008/633/JAI DEL CONSEJO, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, *Diario Oficial de la Unión Europea*, L 218 de 13.8.2008, págs. 129–136. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32008D0633 [consulta: 15 de abril de 2016].

investigación de delitos de terrorismo y de otros delitos graves», tal como el acceso es permitido a Europol, en el marco de su mandato y, siempre que sea necesario, para cumplir sus cometidos[676].

48. En las solicitudes de visados de corta duración (no superiores a noventa días en un periodo de ciento ochenta días) que son admitidas a trámite de acuerdo con el Código de visados, la autoridad responsable de los visados crea un expediente de solicitud, introduciendo en el Sistema de Información sobre Visado VIS, de conformidad con los procedimientos establecidos en el presente Reglamento VIS[677]. El conjunto de datos personales relacionados con el solicitante («*datos alfanuméricos sobre el solicitante y sobre los visados solicitados, expedidos, denegados, anulados, retirados o prorrogados*»; «*fotografías*»; datos relativos a huellas dactilares; vínculos con solicitudes de visado anteriores y expedientes de solicitud de personas que viajan juntas)[678] se transmiten a las autoridades de los Estados miembros responsables de los visados y deben ser tratados con la finalidad exclusiva de adoptar una decisión sobre la solicitud de visado.

49. El acceso al VIS «*para introducir, modificar o suprimir datos*» se limita «*exclusivamente al personal debidamente autorizado de las autoridades competentes*» responsables de la expedición de visados, mientras que el acceso a los efectos de consulta de datos está disponible «*exclusivamente al personal debidamente autorizado de las autoridades*» encargadas de los visados y de «*las autoridades competentes*» en materia de controles en las fronteras exteriores y en los puntos de paso de las fronteras exteriores, controles de inmigración y asilo, y está limitado en la medida en que tales datos sean necesarios para el desempeño de sus funciones[679].

50. Todos los datos personales del solicitante, así como los relativas a la decisión de expedir o denegar un visado solicitado[680] o una eventual decisión de anulación, retirada o de

[676] Artículo 3 (Disponibilidad de los datos para la prevención, detección e investigación de delitos de terrorismo y otros delitos graves) del Reglamento VIS.
[677] *Vid*. «Código de visados», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:jl0028 [consulta: 16 de abril de 2016].
[678] Artículo 5 (Categorías de datos), del Reglamento VIS.
[679] Artículo 6 (Acceso al VIS para introducir, modificar, suprimir y consultar datos), apartados 1 y 2, del Reglamento VIS. Las autoridades con acceso al VIS deben asegurarse de utilizar los datos estrictamente en la medida en que sean necesarios para realizar sus tareas. Asimismo, deben garantizar que al utilizar el VIS no discriminan a los solicitantes o titulares de visado y que respetan plenamente su dignidad humana e integridad. Artículo 7 (Principios generales) del Reglamento VIS.
[680] Las causas de denegación de los visados son las siguientes: carecer de documento de viaje válido; estar «*en posesión de un documento de viaje falso, falsificado o alterado*»; «*no justificar la finalidad y las condiciones de la estancia prevista; no aportar pruebas de que se dispone de medios de subsistencia suficientes para la*

prórroga del periodo de validez de un visado, se introducen y se almacenan en el VIS durante un período máximo de cinco años[681]. En el VIS se insertan los datos personales y biométricos de todos los solicitantes de visado. El VIS «*contiene datos sobre 20 millones de solicitudes de visados, y en horas punta maneja más de 50000 transacciones por hora*». Cada solicitante de visado proporciona información biográfica detallada, una fotografía digital y diez impresiones dactilares. Parece que, de esta forma, «*es un medio fiable para verificar la identidad de los solicitantes de visado, para evaluar los posibles casos de migración irregular y riegos para la seguridad, y para prevenir la búsqueda de visados de conveniencia*»[682].

51. El país responsable proporciona a las personas afectadas la información relativa a la identidad y los datos de contacto del responsable del tratamiento de los datos, la finalidad del tratamiento de los datos en el VIS, las categorías de los destinatarios de los datos, el periodo de almacenamiento de los datos y el derecho de acceso, rectificación y eliminación de los datos. Además, el mismo país deberá informar a las personas implicadas de su obligación de recopilar los datos[683]. Toda persona tiene derecho a recibir información sobre cómo emprender acciones o interponer una demanda ante las autoridades o los tribunales competentes de dicho país si se le deniega el derecho de acceso o el derecho de rectificación o supresión de datos que le afecten[684].

52. Los datos tratados en el VIS no pueden transmitirse a un tercer país u organización internacional salvo que se considere indispensable para probar la identidad de nacionales de terceros países en casos concretos[685].

---

totalidad de la estancia prevista y para el regreso al País de origen o de residencia; haber permanecido ya por tres meses durante el semestre en curso, en el territorio de los Estados miembros con un visado uniforme o un visado de validez territorial limitada»; «*se trata de una persona que esté incluida en la lista de no admisibles en el Sistema de Información de Schengen (SIS) o en el registro nacional; se considera que constituye una amenaza para el orden público, la seguridad interior o las relaciones internacionales de cualquiera de los Estados miembros, o para la salud pública en el sentido del artículo 2, punto 19, del Reglamento (CE) n. 562/2006 del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, por el que se establece un Código comunitario de normas para el cruce de personas por las fronteras (Código de fronteras Schengen)*». Artículo 12 (Datos que se añadirán tras la denegación del visado) del Reglamento VIS.

[681] Artículo 23 (Período de conservación de los datos almacenados) y considerando 14 del Reglamento VIS.

[682] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[683] Artículo 37 (Derecho de información) del Reglamento VIS.

[684] Artículo 38 (Derecho de acceso, corrección y supresión) y artículo 40 (Vías de recurso) del Reglamento VIS.

[685] Artículo 31 (Transmisión de datos a terceros países u organizaciones internacionales) del Reglamento VIS.

53. La unidad central del Sistema de Información de Visados y de las interfaces nacionales[686] son gestionadas, desde el 1 de diciembre de 2012, por *eu-LISA*. Además, con el fin de asegurar una infraestructura de comunicación entre ambas (CS-VIS y NI-VIS), *eu-LISA* se encarga de la supervisión, la seguridad y la coordinación de las relaciones entre los países participantes y el proveedor de servicios. *eu-LISA* también garantiza que el VIS funcione de conformidad con el Reglamento VIS y que únicamente el personal debidamente autorizado tenga acceso a los datos procesados en el VIS.

54. Las actividades de tratamiento de datos de los países incluidos en el sistema son supervisadas por las autoridades nacionales de control, designadas de acuerdo con el nuevo RGPD, que controlen la licitud del tratamiento de los datos de carácter personal por parte de dicho país, en el caso de España se trata de la AEPD. Mientras que las de la Comisión Europea[687] son supervisadas por el SEPD[688], como también el SEPD controla las actividades de *eu-LISA*.

55. Con respecto a las posibilidades que ofrece el marco jurídico actual para acceder a los datos del VIS con fines policiales, «*los Estados miembros aplican estas posibilidades de*

[686] El VIS está conectado a los sistemas nacionales de cada país a través de la interfaz nacional del país en cuestión. Los países participantes designan a la autoridad nacional que se conecta a dicha interfaz nacional y que proporciona acceso al VIS a las autoridades competentes. Los Estados miembros serán responsables: «*del desarrollo*», «*la organización, gestión, funcionamiento y mantenimiento de su sistema nacional*»; de garantizar la seguridad de los datos antes y durante la transmisión a su interfaz nacional, adoptando para ello un «*plan de seguridad*»; de la gestión y las condiciones de acceso al VIS del personal debidamente autorizado de las autoridades nacionales competentes, de conformidad con el presente Reglamento; de los costes correspondientes de los sistemas nacionales. *Vid*. artículo 28 (Relación con los sistemas nacionales) del Reglamento VIS y artículo 32 (Seguridad de los datos).

[687] Recientemente, la Comisión Europea ha pedido reforzar el Sistema de Información de Visados (VIS) para mejorar su interconexión con otras bases de datos, tras concluir que el sistema funciona y contribuye a atajar la inmigración irregular y los riesgos de seguridad. La Comisión ha adoptado un Informe de Evaluación sobre la aplicación del Sistema de Información de Visados (VIS), que analiza, en términos globales, que el uso del Sistema ha acelerado el procesamiento de solicitudes de visados ofreciendo un medio rápido y fiable de verificar el historial de visados de solicitante y de evaluar los riesgos de inmigración irregular y de seguridad. El Informe forma parte del programa "*Regulatory Fitness and Performance* (*REFIT*)" y es el primero de una serie de evaluaciones de los sistemas de información de la UE para las fronteras y la seguridad. La Comisión concluye que el VIS cumple sus objetivos y funciones bien a un coste razonable y tiene un claro valor añadido de la UE. El VIS ayuda a impedir las amenazas al dar a las fuerzas y cuerpos de seguridad del Estado el acceso para consultar el VIS para ayudarles a prevenir, detectar e investigar ofensas terroristas y otros delitos criminales serios. El Sistema, uno de los más avanzados que existen, con cerca de 23 millones de visados solicitados y18,8 millones de huellas dactilares registradas hasta finales de marzo de 2016. EUROPEAN COMMISSION - News (2016), Commission presents REFIT evaluation of the Visa Information System, 14 October 2016. Disponible en Internet: https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20161014_1_en [consulta: 29 de octubre de 2016].

[688] Artículo 42 (Control a cargo del Supervisor Europeo de Protección de Datos) del Reglamento VIS.

forma desigual». En este sentido, «*Estados miembros han notificado problemas prácticos en los procedimientos de acceso al VIS por las autoridades policiales*»[689].

56. La gestión de la migración, la gestión integrada de las fronteras exteriores de la UE y la lucha contra el terrorismo y la delincuencia transfronteriza plantean importantes desafíos y se han vuelto cada vez más complejas en un mundo globalizado. En los últimos años, las instituciones europeas han trabajado en un nuevo enfoque integral para salvaguardar y mantener la seguridad sin comprometer los valores y las libertades fundamentales de la UE. En estos esfuerzos, es clave el intercambio efectivo de información entre las autoridades policiales nacionales, y entre los Estados miembros y las agencias pertinentes de la UE. Se debería superar las deficiencias en las funcionalidades de la gestión de datos fragmentada de la UE entre los diferentes sistemas de información, como SIS II, VIS y Eurodac (*infra*), mediante la exploración del potencial de "interoperabilidad, es decir la capacidad de los sistemas de información para intercambiar datos y permitir el intercambio de información"[690]. El objetivo principal es garantizar que las autoridades policiales, aduaneras y judiciales competentes cuenten sistemáticamente con la "información necesaria para el desempeño de sus funciones, manteniendo al mismo tiempo un equilibrio con respecto a los derechos a la privacidad, la protección de datos y otros derechos fundamentales". Este intercambio no debe comprometer las reglas necesariamente estrictas de acceso y uso garantizadas por el RGPD, la Directiva de protección de datos para asuntos policiales y judiciales, la CDFUE y todas las demás normas pertinentes.

4. Implicaciones del derecho a la protección de datos personales de la obligación de proporcionar huellas dactilares para Eurodac

57. La constante de la amenaza terrorista junto al agravamiento de la crisis migratoria han hecho necesario que las autoridades competentes tengan acceso a información cada vez más completa y actualizada posible para tratar de responder a nivel supranacional a estos fenómenos. En este contexto surge el Sistema de Información Eurodac (en adelante, Eurodac) que fue diseñado para el tratamiento y almacenamiento de registros de huellas dactilares de solicitantes de asilo y refugio. Con posterioridad la información Eurodac se

[689] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.
[690] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

hace accesible también para «*fines de prevención, detección o investigación de los delitos de terrorismo o de otros delitos graves*» bajo el principio de disponibilidad[691].

58. El Sistema de Información Eurodac (abreviatura inglesa de *European Dactyloscopie*), es una base de datos de huellas dactilares europea, que intenta determinar mediante un control de las impresiones dactilares la identidad exacta de las personas[692]. Esta base de datos fue instituida con Reglamento (CE) n. 2725/2000 del Consejo Europeo[693], y en la actualidad se rige por el nuevo y más amplio Reglamento n. 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares (en adelante, Reglamento Eurodac) que entró en vigor el 20 de julio de 2015.

59. Desde su puesta en marcha el 15 de enero de 2003, Eurodac ha conseguido el objetivo de proporcionar pruebas dactilares para facilitar a los Estados miembros responsables el examen de las solicitudes de asilo presentadas en la Unión, y formar parte fundamental del sistema europeo común de asilo de la UE.

---

691 En particular *vid*. considerando 15 del REGLAMENTO (UE) N. 603/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n. 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n. 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (refundición), *Diario Oficial de la Unión Europea*, L 180 de 29.6.2013, págs. 1–30. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32013R0603 [consulta: 02 de mayo de 2016].

692 Alejandro Luis GACITÚA ESPÓSITO (2014: 245).

693 REGLAMENTO (CE) N. 2725/2000 DEL CONSEJO, de 11 de diciembre de 2000, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, *Diario Oficial de la Unión Europea*, L 316 de 15.12.2000, págs. 1–10. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32000R2725 [consulta: 05 de mayo de 2016]; y REGLAMENTO (CE) N. 407/2002 DEL CONSEJO, de 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) n. 2725/2000 relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, *Diario Oficial de la Unión* Europea, L 062 de 05.03.2002, págs. 0001 – 0005. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32002R0407 [consulta: 05 de mayo de 2016]. Al respecto *vid*. Irene CLARO QUINTÁNS (2003), «El sistema "Eurodac" y la identificación de los solicitantes de asilo en la Unión Europea», en María Susana DE TOMÁS MORALES, Christine HELLER DEL RIEGO, y María Esther VAQUERO LAFUENTE (coord.), *El día de Europa: las transformaciones de la Unión Europea: la ampliación y la convención europea: actas de las II jornadas en conmemoración del Día de Europa de la Universidad Pontificia Comillas de Madrid*, Madrid, Universidad Pontificia Comillas, 8 y 9 de mayo de 2003, págs. 215-228; Jonathan P. AUS (2006), «Eurodac: A Solution Looking for a Problem?», en *European integration online papers (EIoP)*, núm. 10, págs. 1-26. Disponible en Internet: http://eiop.or.at/eiop/pdf/2006-006.pdf [consulta: 08 de mayo de 2016]; Blanca GARCÉS-MASCAREÑAS (2015), «Por qué Dublín "no funciona"», en *notes internacionals CIDOB 135*.

60. Eurodac contiene las «*impresiones dactilares de los solicitantes de asilo y los nacionales de terceros países que cruzan ilegalmente las fronteras exteriores*» del Espacio Schengen. Su objetivo principal es «*determinar qué país de la UE es responsable de la tramitación de una solicitud de asilo*», de acuerdo con el Reglamento de Dublín[694]. Está disponible en los pasos fronterizos[695], «*pero a diferencia del SIS y del VIS, no es un sistema de gestión de fronteras*»[696].

61. Sin embargo, la situación cambió a partir de 2015, cuando entró en vigor el Reglamento Eurodac revisado que prevé expresamente el acceso al sistema por parte de los servicios de seguridad de los Estados miembros, aunque bajo condiciones estrictas. El acceso será posible sólo después de la finalización de la consulta (con resultados negativos) de las siguientes bases de datos[697]: bases de datos nacionales de impresión dactilar latente y huella dactiloscópica (ADN), bases de datos de cooperación policial en virtud del Tratado de Prüm y bases de datos del Sistema de Información de Visados (VIS)[698]. Además, la nueva regulación permite el acceso a los datos en el sistema Eurodac también a las autoridades policiales nacionales responsable del terrorismo u otros delitos graves, así como a Europol, con el fin de «*prevenir, detectar o investigar un delito grave o un delito de terrorismo*». La consulta está permitida solamente «*a efectos de prevención, detección o investigación de delitos de terrorismo o de otros delitos graves*», es decir, «*que exista un interés superior de seguridad pública que haga que sea proporcionada la consulta de la base de datos*», pero no para los delitos menores. La comparación debe referirse a casos concretos y no se permiten comparaciones sistemáticas. También, es necesario que «*existan motivos razonables*» para considerar que la comparación con los datos de Eurodac «*contribuirá*

[694] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final. Sobre el Reglamento de Dublín, *vid*. REGLAMENTO (CE) N. 343/2003 DEL CONSEJO, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, *Diario Oficial de la Unión Europea*, L 050 de 25.02.2003, págs. 0001 – 0010. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32003R0343 [consulta: 15 de mayo de 2016].

[695] Eurodac también «*servía para prevenir casos de "shopping de asilo"*» (en inglés "asylum shopping") «*y "refugiados en órbita"*». El primero, «*consiste en solicitar múltiples asilos de manera simultánea por la misma persona en diversos estados miembros. Los "refugiados en órbita" es la situación en la que todos los Estados miembros reclaman que no son competentes para examinar una solicitud de asilo*». *Vid*. Cristina BLASI CASAGRAN (2015: 132).

[696] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[697] Considerando 14 y artículo 20 (Condiciones de acceso a Eurodac por parte de las autoridades designadas) del Reglamento Eurodac.

[698] Considerando 33 del Reglamento Eurodac.

sustancialmente a la prevención, detección o investigación de cualquiera de los delitos en cuestión»[699].

62. El acceso a los datos de Eurodac por parte de las autoridades policiales de los Estado miembros y Europol, encuentra legitimidad en la nueva normativa, que introduce una novedad significativa en cuanto a la finalidad para la que se recogen y examinan los datos. El artículo 1, apartado 2, del Reglamento Eurodac establece que la nueva normativa deberá definir: «*las condiciones en que las autoridades designadas de los Estados miembros y la Oficina Europea de Policía (Europol) podrán solicitar la comparación de datos dactiloscópicos con los almacenados en el Sistema Central de Eurodac a efectos de aplicación de la ley*»[700]. Como subrayó el SEPD, el acceso de las autoridades de policía modifica significativamente el impacto en las vidas de las personas vulnerables y con necesidad de protección, tanto que la evaluación de la necesidad y la proporcionalidad de la creación de Eurodac habría sido completamente diferente si se hubiese contemplado desde un principio este acceso de las autoridades policiales. El Reglamento Eurodac hace surgir un nuevo régimen jurídico, en el que se recopilarán datos para examinar las solicitudes de asilo, pero los datos podrían utilizarse, en determinadas circunstancias, con otro fin, es decir, la aplicación de la ley fuera del contexto del asilo y la migración. Esto constituye lo que a menudo se describe como "desviación de uso" ("*function creep*"), es decir, una extensión gradual del uso de un sistema o base de datos más allá del propósito para el cual fue originalmente pensado[701].

63. La recopilación de datos con una finalidad (en el caso concreto, la determinación del Estado responsable de la solicitud de asilo) y la posterior ampliación de las posibilidades de utilización de los datos recogidos tienen "un impacto importante en la protección de los datos personales". Estos factores también parecen ser críticos en el respeto de los principios de necesidad y proporcionalidad exigidos por la ley para derogar el principio de la limitación

[699] Artículo 21 (Condiciones de acceso a Eurodac por parte de Europol) del Reglamento Eurodac. Existirán motivos razonables, en particular, «*cuando haya una sospecha fundada de que el sospechoso, el autor o la víctima de un delito de terrorismo o de otro delito grave están encuadrados en una categoría contemplada*» en el Reglamento Eurodac.

[700] Artículo 1 (Finalidad de «Eurodac»), apartado 1, del Reglamento Eurodac: «*Se crea un sistema denominado «Eurodac», cuya finalidad será ayudar a determinar el Estado miembro responsable, con arreglo al Reglamento (UE) nº 604/2013 del examen de las solicitudes de protección internacional presentadas en los Estados miembros por un nacional de un tercer país o un apátrida y, además, facilitar la aplicación del Reglamento (UE) nº 604/2013 en las condiciones establecidas en el presente Reglamento*».

[701] EUROPEAN DATA PROTECTION SUPERVISOR (2012: 7).

de la función en la protección de datos personales. Nos enfrentamos a un sistema de control amplio y generalizado[702].

64. El Reglamento Eurodac también prevé (Capítulo VII - Tratamiento de los datos, protección de los datos y responsabilidad) una serie de disposiciones sobre la responsabilidad en materia de tratamiento de datos, transmisión de datos y modalidad para llevar a cabo las comparaciones y la transmisión de resultados, derechos del sujeto de los datos, la supervisión a nivel nacional de las autoridades nacionales de control, mientras que las de la Comisión son supervisadas por el SEPD[703], además sobre la seguridad de los datos y sobre la prohibición de la transferencia a terceros países, organizaciones internacionales o personas privadas[704]. En este sentido, los países de la UE[705] que mandan datos a Eurodac tienen que garantizar que las huellas sean registradas de acuerdo con la ley y que, siempre dentro del respeto de la legalidad, se desarrollen las operaciones de tratamiento, transmisión, almacenamiento o eliminación de los datos[706].

65. Además, está prevista una primera evaluación de este Reglamento Eurodac por la Comisión Europea (a mediados de 2018) sobre los resultados obtenidos en relación con los objetivos y el impacto sobre los derechos fundamentales[707]. Los Estados miembros y

[702] EUROPEAN DATA PROTECTION SUPERVISOR (2012: 7-10).

[703] Sobre la propuesta de Reglamento Eurodac, el SEPD había expresado, como comentamos arriba, muchas críticas con respecto al uso de los sistemas de bases de datos que van más allá de la finalidad para la que fueron pensados originalmente. En particular, el Supervisor reaccionó «*frente a este hecho y se quejó de que la Comisión no había demostrado suficientemente que las huellas dactilares de los solicitantes de asilo podían ser necesarias para investigaciones policiales. Por eso, pidió a la Comisión que proporcionara pruebas sólidas y estadísticas fiables sobre la necesidad de acceder a los datos de Eurodac*». En Cristina BLASI CASAGRAN (2015: 145). *Amplius*, EUROPEAN DATA PROTECTION SUPERVISOR (2012). Siguiendo con las críticas al Reglamento Eurodac, *vid*. también Chris JONES (2014), «Analysis 11 Years of Eurodac», en *Statewatch News Online*, págs. 17. Disponible en Internet: http://database.statewatch.org/article.asp?aid=33094 [consulta: 25 de mayo de 2016].

[704] Artículo 35 (Prohibición de transferencia de datos a terceros países, organismos internacionales o particulares) del Reglamento Eurodac.

[705] Las nuevas disposiciones del Reglamento sobre el acceso de las autoridades policiales no constituyen un desarrollo del *acquis* de Schengen y, por tanto, no se aplican automáticamente a Suiza, Irlanda y Dinamarca. Para garantizar el acceso será necesario concluir un acuerdo específico con la UE.

[706] *Vid*. *amplius*, Capítulo VII (Tratamiento de los datos, protección de los datos y responsabilidad) del Reglamento Eurodac.

[707] *Vid*. «Il nuovo Regolamento Eurodac (603/2013) per la raccolta e comparazione delle impronte digitali si applica a partire da oggi», en *Asilo in Europa*, 20 luglio 2015. Disponible en Internet: http://www.asiloineuropa.it/2015/07/20/il-nuovo-regolamento-eurodac-6032013-per-la-raccolta-e-comparazione-delle-impronte-digitali-si-applica-a-partire-da-oggi/ [consulta: 28 de mayo de 2016]. En octubre de 2015, la Agencia Europea de Derechos Fundamentales intervine sobre las implicaciones de los derechos fundamentales de la obligación de proporcionar huellas dactilares para su inclusión en el Sistema Eurodac. *Vid*. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2015), *Fundamental rights implications of the obligation to provide fingerprints for Eurodac*, Vienna, Publications Office, págs. 12. Disponible en Internet: http://fra.europa.eu/en/publication/2015/fundamental-rights-implications-obligation-provide-fingerprints-eurodac [consulta: 29 de mayo de 2016].

Europol deben llevar a cabo un informe anual «*sobre la eficacia de la comparación de los datos*» relativos a las huellas dactiloscópicas con datos Eurodac a los efectos de la lucha contra el terrorismo u otros delitos graves[708].

66. «*Desde hace varios años, Europa se enfrenta a una profunda crisis migratoria y de refugiados*» que, desde 2015, no hace sino agravarse cada vez más. En consecuencia, la Comisión Europea «*propuso la reforma del Reglamento de Dublín, con el fin de adaptarlo a la situación actual*»[709]. También la Comisión, en mayo de 2016, cuando el Reglamento Europol de 2013 había entrado en vigor y aún no estaba plenamente operativo - con la consiguiente imposibilidad de evaluar sus efectos - propuso igualmente una refundición del Reglamento Eurodac[710].

67. El principal cambio contenido en esta propuesta de Reglamento[711] consiste «*en ampliar el ámbito de aplicación de Eurodac a fin de registrar a los nacionales de terceros países que se encuentren ilegalmente en un Estado miembro o que sean detenidos al cruzar irregularmente las fronteras de un Estado miembro con un tercer país*»[712].

---

[708] Artículo 40 (Informe anual, seguimiento y evaluación) del Reglamento Eurodac.

[709] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo (Reglamentos Eurodac, EASO y Dublín), *Diario Oficial de la Unión Europea*, C 9 de 12.1.2017, págs. 3–5. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017XX0112(01)&qid=1504086633377#ntc4-C_2017009ES.01000301-E0004 [consulta: 08 de agosto de 2017]. «*Esta reforma va unida a la propuesta de creación de una Agencia de Asilo de la Unión Europea, cuya misión será ayudar a los Estados miembros a cumplir sus obligaciones en materia de asilo*».

[710] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo. PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n. 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida] y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (refundición), COM(2016) 272 final - 2016/0132 (COD), Bruselas, 4.5.2016. Disponible en Internet: https://ec.europa.eu/transparency/regdoc/rep/1/2016/ES/1-2016-272-ES-F1-1.PDF [consulta: 02 de junio de 2016].

[711] En el momento de la redacción de la tesis, los debates sobre la propuesta en el Parlamento y el Consejo estaban en curso. *Vid*. INFORME SOBRE LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (versión refundida) (COM(2016)0272 – C8-0179/2016 – 2016/0132(COD)), 9 de junio de 2017.

[712] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo. Artículo 1 (Finalidad de

68. Dicha propuesta está en consonancia con los objetivos anunciados en la Comunicación de la Comisión titulada "Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad"[713] y, en este sentido, «*conforma Eurodac de manera que en el futuro sea posible, cuando sea necesaria y proporcionada, la interoperabilidad con otros sistemas de información*». A tal fin, «*la Comisión evaluará la necesidad y proporcionalidad de establecer la interoperabilidad con el Sistema de Información de Schengen (SIS) y el Sistema de Información de Visados (VIS)*». La propuesta de Reglamento «*hará posible que los servicios de seguridad y Europol tengan acceso a toda la información conservada en el sistema y efectúen en el futuro búsquedas basadas en una imagen facial*»[714].

69. Entre los aspectos más relevantes desde el punto de vista de las investigaciones y los procesos penales, está la posibilidad de facilitar a las autoridades policiales un acceso más amplio al Sistema de Información Eurodac y en simplificar las modalidades de acceso a dicho sistema[715]. Este mayor acceso policial es significativo porque en los años posteriores a la creación del sistema la posición prácticamente unánime entre los Estados miembros y las instituciones UE (de manera especial el SEPD) fue que Eurodac únicamente debería ser consultada por las autoridades administrativas competentes para resolver las peticiones de asilo, y no para finalidades distintas como podrían ser la prevención y lucha contra la criminalidad[716].

«Eurodac»), letra b) de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares.

[713] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[714] PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares, pág. 5.

[715] *Amplius vid*. SERVIZIO STUDI DEL SENATO (2016b), «Proposta di Regolamento del Parlamento Europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di paese terzo o da un apolide, per l'identificazione di cittadini di paesi terzi o apolidi il cui soggiorno è irregolare e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto (rifusione)», en *Note su atti dell'Unione europea*, núm. 67, págs. 10. Disponible en Internet: https://www.senato.it/service/PDF/PDFServer/BGT/00989852.pdf [consulta: 05 de junio de 2017]; Valeria FERRARIS (2017), «Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste», en *Diritto, Immigrazione e Cittadinanza*, núm. 2, págs. 16. Disponible en Internet: https://www.dirittoimmigrazionecittadinanza.it/archivio-saggi-commenti/saggi/fascicolo-2017-n-2/128-eurodac-e-i-limiti-della-legge-quando-il-diritto-alla-protezione-dei-dati-personali-non-esiste [consulta: 01 de agosto de 2017].

[716] La propuesta de Reglamento prevé que el sistema se utilice para ayudar a controlar la inmigración ilegal y los desplazamientos secundarios de ciudadanos de terceros países dentro de la Unión Europea e identificar a los ciudadanos de terceros países ilegalmente presentes para ayudar a los países europeos an determinar las medidas apropiadas que deben adoptarse contra ellos, incluida la repatriación de los que están presentes sin autorización.

70. De este modo, Eurodac pasaría a ser «*una base de datos para fines generales de inmigración y ya no se limitaría a garantizar la aplicación efectiva del Reglamento Dublín III, aunque esta función seguirá siendo uno de sus aspectos importantes*». La ampliación del ámbito de aplicación de Eurodac permitirá a las autoridades competentes en materia de inmigración de un Estado miembro transmitir y comparar los datos relativos a los nacionales de terceros países en situación ilegal que no solicitan asilo y que pueden circular dentro de la Unión Europea sin ser detectados[717].

71. Esta ampliación del «*ámbito de aplicación de Eurodac plantea objeciones respecto al principio de limitación a una finalidad específica consagrado en el artículo 7 de la CDFUE*»[718] (que es la protección contra el terrorismo u otros delitos graves o control de los movimientos secundarios y lucha contra la inmigración irregular), sin tener en cuenta la necesidad y proporcionalidad de esta extensión que modifica radicalmente el significado del instrumento.

72. También, en la propuesta de Reglamento de la Comisión a la conservación de los datos personales de los sujetos interesados establecidos en la normativa actual, se añaden las imágenes faciales[719], además de los datos anagráficos y la nacionalidad, perdiendo así Eurodac la característica de una base de datos que no contiene datos anagráficos del sujeto registrado[720]. La propuesta de Reglamento «*no hace referencia a evaluación alguna de la*

[717] PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares, pág. 12.

[718] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo.

[719] Artículo 2 (Obligación de tomar las impresiones dactilares y una imagen facial) de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares: «*Los Estados miembros tienen la obligación de tomar las impresiones dactilares y una imagen facial de las personas* (…) *e impondrán al sujeto de los datos la obligación de facilitar sus impresiones dactilares y una imagen facial y de informarles al respecto* (…)». «*Los datos dactiloscópicos y los datos de imagen facial transmitidos por cualquier Estado miembro, se compararán automáticamente con los datos dactiloscópicos transmitidos por otros Estados miembros y ya conservados en el Sistema Central*». Artículo 15 (Comparación de los datos dactiloscópicos y los datos de imagen facial) de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares.

[720] Artículo 12 (Registro de datos) de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares: «*En el Sistema Central se registrarán exclusivamente los datos siguientes: a) datos dactiloscópicos; b) una imagen facial; c) nombre o nombres y apellido o apellidos, nombre o nombres de nacimiento y nombres usados con anterioridad, así como cualquier alias, que podrán consignarse separadamente; d) nacionalidad o nacionalidades; e) lugar y fecha de nacimiento; f) Estado miembro de origen, lugar y fecha de la solicitud de protección internacional* (…)*;* la *fecha de solicitud será la introducida por el Estado miembro que trasladó al solicitante; g) sexo; h) tipo y número del documento de identidad o del documento de viaje; código de tres letras del país expedidor y período de validez* (…)».

necesidad de recopilar y utilizar imágenes faciales de las categorías de personas que se recogen en la propuesta de refundición del Reglamento Eurodac»[721].

73. El artículo 17 de la propuesta de Reglamento, sin cambios con la anterior normativa, prevé que los datos relativos a un solicitante de protección internacional permanecerán diez años, sin embargo, los datos sobre los nacionales de terceros países en estancia irregular se mantendrán durante un período de cinco años. A este respecto resulta interesante las conclusiones del SEPD que recomienda «*bloquear todos los datos para fines de seguridad pública al cabo de tres años, y que deje de efectuarse una distinción entre las distintas categorías de nacionales de terceros países a este respecto*»[722].

74. El actual Reglamento Eurodac como también la propuesta de Reglamento, prohíben rigurosamente las transferencias de datos personales con «*terceros países, organizaciones internacionales entidades privadas establecidas dentro o fuera de la Unión*» (considerando 41). Considerada la ampliación del ámbito de aplicación de Eurodac por la propuesta, se introdujo una nueva disposición específica para la transferencia de datos personales a terceros países «*en caso necesario con el fin de probar la identidad de los nacionales de terceros países a efectos de retorno*»[723]. Sin embargo, prohíbe a un tercer país, al que no se aplique el Reglamento de Dublín, consultar la base de datos de Eurodac o que un Estado miembro pueda realizar controles en la base de datos en nombre de un tercer País.

75. Por último, en virtud del Reglamento (UE) n. 603/2013, también confirmado por la nueva propuesta, pasa a ser responsable de la gestión operativa de Eurodac la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (*eu-LISA*)[724] que, además de de Eurodac, es responsable de

[721] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo.
[722] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo.
[723] Artículo 38 (Transferencia de datos a terceros países a efectos de retorno), apartado 1 de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares, COM(2016) 272 final - 2016/0132 (COD).
[724] REGLAMENTO (UE) N. 1077/2011 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, *Diario Oficial de la Unión Europea*, L 286 de 1.11.2011, págs. 1-17. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2011.286.01.0001.01.SPA&toc=OJ:L:2011:286:TOC [consulta: 08 de junio de 2016]. En particular, *vid*. artículo 5 (Funciones relacionadas con Eurodac). Hay que recordar que estas funciones ahora son llevadas a cabo por la nueva Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (*eu-LISA*), creada por el Reglamento (UE) 2018/1726 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018.

la gestión del Sistema de Información de Visados (VIS) y el Sistema de Información de Schengen de segunda generación (SIS II) con el fin de garantizar un intercambio permanente, seguro y continuo de información y datos entre los Estados miembros. Pero la propuesta va más allá, permitiendo a *eu-LISA* «*utilizar datos personales reales de Eurodac para realizar ensayos*» en las siguientes circunstancias: a efectos de «*diagnóstico y reparación, cuando se descubran defectos en el Sistema Central*»; «*para someter a ensayo nuevas tecnologías y técnicas pertinentes con el fin de mejorar el rendimiento del Sistema Central o la transmisión de datos al mismo*»[725]. Sobre esta previsión, el SEPD es muy crítico incluso expresando «*graves inquietudes y el Reglamento Eurodac no debería permitirlo*», añadiendo que el legislador debería «*estudiar y evaluar la alternativa de usar datos ficticios, en vista del riesgo para la vida privada de las personas interesadas*»[726].

76. En tanto que la UE debe hacer frente a los retos que plantea la crisis migratoria y de refugiados, y resulta necesario que «*cuente con una política eficaz y armonizada para hacer frente a la inmigración irregular que tiene lugar tanto dentro de la Unión como en dirección a la misma*», la ampliación del ámbito de aplicación de Eurodac plantea *in primis*, como ya se ha comentado, «*objeciones respecto al principio de limitación a una finalidad específica consagrado en el artículo 7 de la CDFUE*». También sobre la inclusión de las imágenes faciales, «*el Reglamento no hace referencia a evaluación alguna de la necesidad de recopilar y utilizar imágenes faciales de las categorías de personas que se recogen en la propuesta de refundición del Reglamento Eurodac*». En el texto de la propuesta, falta la indicación de que «*la responsabilidad en última instancia del tratamiento de datos personales corresponderá a los Estados miembros, que se considerarán responsables del tratamiento*» en el sentido del RGPD.

77. Por último, en relación con las novedades de la propuesta de Reglamento Eurodac, y por lo que interesa al objeto de la presente investigación, sería recomendable que «*el acceso de las autoridades encargadas de velar por la seguridad pública fuese evaluado por un órgano independiente*». Por el contrario, «*las autoridades designadas y las autoridades de*

[725] Artículo 5 (Gestión operativa) de la PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares, COM(2016) 272 final - 2016/0132 (COD).

[726] Siempre el SEPD en su Resume, en relación con el tratamiento de información por parte de *eu-LISA*, recomienda adoptar salvaguardias adecuadas en relación con el acceso a los datos por parte de contratistas externos. *Vid*. RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo.

verificación no deberían formar parte de la misma organización a fin de mantener la independencia de las autoridades responsables de la verificación»[727].

78. Así planteadas las cosas, resulta evidente que un instrumento administrativo accesorio a la regulación del sistema de asilo como Eurodac pasaría a convertirse, con la nueva propuesta, en una herramienta de control de los Estado sobre una población en particular pertenecientes a grupos vulnerables que requieren de protección específica, como los migrantes y los refugiados, que suelen carecer de mecanismos de defensa de sus derechos e intereses, en particular, por lo que se refiere al tratamiento de datos personales.

5. La Decisión Prüm y lucha contra el terrorismo: ¿existe la protección de los derechos fundamentales en Europa?

79. Desde hace años Europa ha señalado, como eje central para la lucha contra el crimen organizado y el terrorismo, la necesidad de mejorar la cooperación transnacional, diseñada específicamente para equilibrar y fortalecer dicha cooperación y garantizar en todo momento la protección de los datos personales. Sin embargo, fuera del contexto de la Unión Europea, siete Estados miembros de la misma UE firmaron un acuerdo multilateral, el Tratado de Prüm, de 27 de mayo de 2005, sobre profundización de la cooperación transfronteriza, en particular, "para combatir el terrorismo, la delincuencia transfronteriza y la migración ilegal, aceptando el principio de disponibilidad de la información con el fin de hacer más eficaz la cooperación entre las autoridades nacionales responsables de la actividad de prevención de la delincuencia transnacional"[728].

---

[727] RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo.

[728] «*El Tratado de Prüm se concluyó el 27 de mayo de 2005 en Prüm (Alemania); lo firmaron siete Estados miembros (Bélgica, Alemania, España, Francia, Luxemburgo, Países Bajos y Austria) y entró en vigor en Austria y España el 1 de noviembre de 2006 y en Alemania el 23 de noviembre de 2006. Otros ocho Estados miembros (Bulgaria, Grecia, Italia, Portugal, Rumanía, Eslovenia, Finlandia y Suecia) han declarado oficialmente su intención de adherirse al mismo. El Tratado establece un marco legal para profundizar la cooperación entre los Estados miembros en la lucha contra el terrorismo, la delincuencia transfronteriza y la inmigración ilegal. Más concretamente, prevé el intercambio entre las Partes contratantes de perfiles de ADN, datos dactiloscópicos, registros de matriculación de vehículos y datos personales y no personales relacionados con la cooperación policial transfronteriza*». En DOCUMENTO DE TRABAJO sobre una Decisión del Consejo relativa a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, 10.4.2007, págs. 6. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824es.pdf [consulta: 19 de octubre de 2015]. Para un estudio más exhaustivo y detallado sobre el Tratado de Prüm, véase los Estudios de los siguientes autores: Teresa FREIXES SANJUÁN (2007); Jacques ZILLER (2007), «El Tratado de Prüm»; Cristina DIETRICH PLAZA (2007), «El Tratado de Prüm en el marco de la regulación de la protección

80. Por sus características, que requiere una "cooperación reforzada"[729] iniciada por los Acuerdos de Schengen, el Tratado de Prüm también se conoce como Schengen III[730]. Si bien las cooperaciones reforzadas en materia penal no se llevaron «*a cabo en los términos procedimentales previstos en el Tratado de Ámsterdam y posteriormente en el Tratado de Niza, lo cierto es que han existido cooperaciones de perfil muy similar*» a estas desarrolladas a través del acervo Schengen y el Tratado de Prüm. Desde la experiencia acumulada se puede afirmar que se trata de «*valiosos instrumentos de avance que, si bien en un primer momento pudieran haber sido fuente de particularismos, lo cierto es que al haberse integrado en el Derecho de la Unión ambos Tratados, no han supuesto perjuicio alguno a la deseada uniformidad jurídica y han procurado importantes avances en la consecución de la*

de datos personales en la Unión Europea»; Emilio ACED FÉLEZ (2007), «Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm»; Gregorio CÁMARA VILLAR (2007), «La garantía de los derechos fundamentales afectados por la Convención de Prüm»; Joan Lluis PÉREZ FRANCESCH (2007), «Cooperación policial y judicial en la Convención de Prüm»; Yolanda GÓMEZ SÁNCHEZ (2007), «Los datos genéticos en el Tratado de Prüm»; Esperanza ZAMBRANO GÓMEZ (2007), «La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm. La perspectiva de las autoridades nacionales de protección de datos»; José Carlos REMOTTI CARBONELL (2007), «Las medidas contra el terrorismo en el marco del Tratado de Prüm»; Antonio ROVIRA (2007), «Los defensores del pueblo y la Convención de Prüm»; Antonio BAR CENDÓN (2007), «El Tratado de Prüm y la inmigración ilegal», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 11-273. ISSN: 1698-4889. Disponible en Internet: http://www.ugr.es/~redce/REDCE7pdf/ReDCE7.pdf [consulta: 19 de octubre de 2015]; Francesco COSTAMAGNA (2010), «Banche dati del Dna e lotta contro il crimine: quale tutela per i diritti fondamentali in Europa?», en *ISPI - Policy Brief*, núm. 197, págs. 10. Disponible en Internet: http://www.ispionline.it/it/documents/PB_197_2010.pdf [consulta: 28 de octubre de 2015]; Óscar JAIME-JIMÉNEZ, Lorenzo CASTRO MORAL (2010), «La criminalidad organizada en la Unión Europea. Estado de la cuestión y respuestas institucionales», en *Revista CIDOB d´Afers Internacionals*, núm. 91, págs. 173-194. Disponible en Internet: http://www.raco.cat/index.php/revistacidob/article/viewFile/211125/280787 [consulta: 28 de octubre de 2015]. Instrumento de ratificación de España del Convenio relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, hecho en Prüm el 27 de mayo de 2005, *Boletín Oficial del Estado*, núm. 307, lunes 25 diciembre 2006, págs. 45524-45534. Por ley núm. 85 de 30 de junio de 2009, Italia ha autorizado la ratificación del Tratado de Prüm y ha previsto la creación de una base de datos nacional de ADN y de un laboratorio central. *Vid*. Legge 30 giugno 2009, n. 85, *Gazzetta Ufficiale*, n. 160 del 13-7-2009 - Suppl. Ordinario n. 108.

[729] Artículo 20 (antiguos artículos 27 A a 27 E, 40 a 40 B y 43 a 45 TUE y antiguos artículos 11 y 11 A TCE): «*1. Los Estados miembros que deseen instaurar entre sí una cooperación reforzada en el marco de las competencias no exclusivas de la Unión podrán hacer uso de las instituciones de ésta y ejercer dichas competencias aplicando las disposiciones pertinentes de los Tratados, dentro de los límites y con arreglo a las modalidades contempladas en el presente artículo y en los artículos 326 a 334 del Tratado de Funcionamiento de la Unión Europea. La finalidad de las cooperaciones reforzadas será impulsar los objetivos de la Unión, proteger sus intereses y reforzar su proceso de integración. Las cooperaciones reforzadas estarán abiertas permanentemente a todos los Estados miembros, de conformidad con el artículo 328 del Tratado de Funcionamiento de la Unión Europea*». En VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA. Sobre este aspecto, *vid*. Giandonato CAGGIANO (2007), «L'evoluzione dello Spazio di libertà, sicurezza e giustizia nella prospettiva di un'Unione basata sul diritto», en *Studi sull'integrazione europea*, núm. 2, pp. 345-348. Disponible en Internet: http://www.studisullintegrazioneeuropea.eu/Scarico/Rivista%20Studi%200207.pdf [consulta: 10 de septiembre de 2017].

[730] Constituye la tercera fase de desarrollo del Acuerdo de Schengen de 1985 (Schengen I) y el Convenio de Aplicación de Schengen 1990 (Schengen II).

supresión de fronteras y los objetivos de seguridad y lucha contra la delincuencia»[731]. Sin embargo, es una elección que tiene claros efectos negativos en términos de transparencia, confianza mutua entre los Estados miembros y coherencia de la acción de la UE en el ámbito de la seguridad[732].

81. El Tratado de Prüm se incorporó a la legislación de la Unión Europea a través de la Decisión 2008/615/JAI del Consejo[733] (en adelante, Decisión Prüm), que subraya la importancia, con el fin de lograr una cooperación internacional eficiente, para intercambiar información precisa con rapidez y eficacia "a fin de prevenir y combatir la delincuencia en tres ámbitos: terrorismo, delincuencia transfronteriza y migración ilegal"[734]. Concretamente, y para alcanzar estos fines, su contenido se centra en el intercambio automatizado de información sobre acontecimientos importantes y con fines de lucha antiterrorista, así como otras formas de cooperación policial transfronteriza. Todo ello sin olvidar que la Decisión

[731] Esther M. ANÍBARRO MARTÍNEZ (2016: 216). Acerca el Tratado de Prüm, Antonella MARANDOLA (2009), «Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione», en Francesco PERONI, Mitja GIALUZ (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT - Edizioni Università di Trieste, págs. 164-189. Disponible en Internet: https://www.openstarts.units.it/dspace/handle/10077/3352 [consulta: 21 de febrero de 2015]; Fernando MARTÍNEZ PÉREZ y María POZA CISNEROS (2013b), «El principio de Disponibilidad: antecedentes penales y Convenio de Prüm», en Miguel CARMONA RUANO, Ignacio U. GONZÁLEZ VEGA, Víctor MORENO CATENA (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 417-496.

[732] En este sentido, *vid*. Thierry BALZACQ, Didier BIGO, Sergio CARRERA, Elspeth GUILD (2006), «Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats», en *CEPS Working Document*, núm. 234, págs. 17-18. Disponible en Internet: https://www.ceps.eu/publications/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats [consulta: 25 de febrero de 2015]. Se considera que Prüm crea una jerarquía en el interior de la UE y que genera potencialmente una competición, por lo que se refiere al intercambio de datos, con el principio de disponibilidad previsto por el Programa de La Haya. Es decir, el Tratado de Prüm debilita a la Unión Europea, porque no tiene la capacidad de establecer un eficiente modelo para la adopción de policías de seguridad, faltando la necesaria coherencia de la acción y minando la confianza de los Estados miembros al desarrollar nuevas políticas de seguridad que operan por encima y desde abajo del nivel europeo, chocando así con el principio de transparencia, estableciendo un marco cuyas reglas no están sujeta al control del Parlamento Europeo. También se señala que el Tratado de Prüm, si bien responde a demandas legítimas, constituye una violación del principio de cooperación leal, que afecta negativamente a la realización del Espacio de Libertad, Seguridad y Justicia.

[733] DECISIÓN 2008/615/JAI DEL CONSEJO, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, L 210 de 6.8.2008, págs. 1–11. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008D0615 [consulta: 09 de julio de 2015]. *Cfr*. el considerando 1 de la Decisión.

[734] «*Se trata de un tratado internacional entre Alemania, Francia, España, Austria y los tres Estados del Benelux para la profundización en la cooperación transfronteriza con el objetivo de combatir el terrorismo, la criminalidad y la inmigración ilegal entre esos Estados. Pretende, pues, profundizar en la consecución de objetivos propios del ELSJ ya previstos en los tratados constitutivos, pero bajo un marco jurídico e institucional ajeno al comunitario. En concreto, su objetivo fundamental es lograr un intercambio más eficiente de información entre los Estados afectados para combatir la criminalidad en un espacio sin fronteras interiores. Tal intercambio de información prevé, por ejemplo, elementos tan sensibles como el acceso on line a datos de ADN, huellas digitales o matrículas de vehículos, a la par que llegado el caso podría conllevar por ejemplo la prohibición de viaje en casos de acontecimientos deportivos o manifestaciones políticas como las reuniones G-8*». En Esther M. ANÍBARRO MARTÍNEZ (2016: 215-216) y José MARTÍN Y PÉREZ DE NANCLARES (2007: 70).

Prüm también reconoce como uno de sus objetivos garantizar un nivel adecuado de protección de los datos personales[735]. Tanto el Tratado de Prüm, que tiene su origen en el Programa de la Haya[736] (*vid*. *supra*), como la Decisión Prüm tienen por fin poner en práctica el "principio de disponibilidad" de la información. En su virtud, «*significa que el agente de los servicios de seguridad de un Estado miembro de la Unión que necesite información para llevar a cabo sus funciones debe poder obtenerla de otro Estado miembro, y que las autoridades de los servicios de seguridad del Estado miembro que tenga dicha información deben ponerla a su disposición para el fin declarado, teniendo en cuenta las necesidades de las investigaciones pendientes en dicho Estado miembro*»[737].

82. Su régimen se contiene en las Decisiones 2008/615/JAI y 2008/616/JAI[738], que son dos instrumentos[739] que prevén la institución, en cada Estado miembro, de una red de bases de datos nacionales de los perfiles de ADN, huellas dactilares y registros de «*matriculación de vehículos*»[740]; el «*suministro de datos relacionados con acontecimientos importantes que tengan una dimensión transfronteriza*»[741]; el «*suministro de información con el fin de*

[735] Capítulo 6 (Disposiciones generales sobre protección de datos) de la Decisión Prüm.
[736] Las conclusiones del Consejo Europeo de Tampere de octubre de 1999 confirmaron la necesidad de mejorar el intercambio de información entre las autoridades policiales de los países de la UE, y el Programa de La Haya volvió a corroborarla en noviembre de 2004.
[737] El "principio de disponibilidad" se puede encuentrar en el considerando 4 de Decisión Prüm. DECISIÓN 2008/615/JAI DEL CONSEJO, de 23 de junio de 2008. Ante dicha Decisión, el Consejo Europeo codificó el "principio de disponibilidad" de la información que estableció un sistema simplificado de «*intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea*» que, no obstante, no impone imperativamente el intercambio de ese tipo de información, pero sí facilita su transmisión entre los servicios de seguridad. También se creó una base de datos conectada con la policía, eficaz sobre el papel: el Sistema de Información Schengen (SIS). *Cfr*. DECISIÓN MARCO 2006/960/JAI DEL CONSEJO, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, *Diario Oficial de la Unión Europea*, L 386 de 29.12.2006, págs. 89–100. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006F0960 [consulta: 09 de julio de 2015]. *Vid*, además, Stefano CIAMPI (2009: 42-44). Al respecto véase José Francisco ETXEBERRIA GURIDI (2009); Emilio ACED FÉLEZ (2010a); del mismo autor en el mismo año, «Principio de disponibilidad y protección de datos en el ámbito policial», en *Noticias Jurídicas*. Disponible en Internet: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4537-principio-de-disponibilidad-y-proteccion-de-datos-en-el-ambito-policial-/ [consulta: 13 de julio de 2015].
[738] DECISIÓN 2008/616/JAI DEL CONSEJO, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, L 210 de 6.8.2008, págs. 12–72. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008D0616 [consulta: 14 de julio de 2015].
[739] Fernando MARTÍNEZ PÉREZ y María POZA CISNEROS (2013b: 437 y ss.).
[740] En particular *vid*. Capítulo 2 (Acceso en línea y solicitudes de seguimiento) de la Decisión Prüm.
[741] Capítulo 3 (Acontecimientos importantes) de la Decisión Prüm.

prevenir atentados terroristas»[742]; junto a «*otras medidas de intensificación de la cooperación policial transfronteriza*»[743].

83. Más concretamente, y por lo que respecta al tema de esta investigación, interesa destacar que la Decisión Prüm, además de prever la creación de ficheros nacionales de análisis del ADN a tres años de su entrada en vigor[744], obliga a los Estados miembros a facilitar los datos de índices contenidos en los ficheros nacionales de análisis del ADN[745], para facilitar el intercambio de información. Se prevé que las autoridades nacionales tendrán acceso a las bases de datos de otros Estados, con el fin de realizar consultas automatizadas mediante la comparación de perfiles de ADN[746].

84. El intercambio de información que los Estados miembros se conceden mutuamente – «*acceso a sus respectivos ficheros automatizados de análisis de ADN, sistemas automatizados de identificación dactiloscópica y datos de los registros de matriculación de vehículos*»[747] –, se basa en el principio de disponibilidad y se divide en dos fases: primero se lanza una búsqueda para determinar si la muestra en cuestión se encuentra en las bases de datos nacionales de los demás Estados miembros («*hit/no hit*») a través de una comparación automática sin el intercambio de datos personales; en caso de un cotejo positivo, el intercambio de datos personales puede ser necesario a través de canales oficiales o procedimientos de asistencia mutua. Este concepto «*se basa en la interconexión de un sistema nacional con los sistemas nacionales de todos los demás Estados miembros de la UE, a fin de permitir la búsqueda cruzada remota. Cuando una búsqueda genera un resultado positivo en la base de datos de otros Estados miembros, los detalles del resultado positivo se intercambian a través de mecanismos bilaterales*»[748].

---

[742] Capítulo 4 (Medidas para la prevención de atentados terroristas) de la Decisión Prüm. «*La transmisión de información para la prevención de atentados vía Europol y Eurojust, donde se faculta a los Países signatarios para que, en casos concretos y sin necesidad de petición previa, puedan transmitirse determinados datos de carácter personal e información en la medida en que se den hechos que permitan justificar la presunción de que las personas afectadas por la medida van a cometer un atentado terrorista*». Alberto PÉREZ DÍAZ-HEREDERO (2016), «La evolución de la Estrategia Antiterrorista europea: Europol y sus grandes retos», en *Análisis GESI*, análisis 30. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5684301 [consulta: 10 de julio de 2017]. Interesante destacar que se proporcionan obligaciones específicas con respecto al intercambio de información entre los Estados miembros y la posibilidad de presencia en aviones de línea de oficiales de policía encargados de garantizar la seguridad en los aviones ("*air marshals*").

[743] Capítulo 5 (Otras formas de cooperación) de la Decisión Prüm.

[744] Artículo 36, apartado 1 (Aplicación y declaraciones) de la Decisión Prüm.

[745] Artículo 2 (Creación de ficheros nacionales de análisis del ADN) de la Decisión Prüm.

[746] Artículo 3 (Consulta automatizada de los perfiles de ADN) de la Decisión Prüm.

[747] Considerando 10 de la Decisión Prüm.

[748] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

85. El artículo 4 de la Decisión Prüm también prevé la posibilidad de una comparación automática entre los «*perfiles de ADN no identificados con todos los perfiles de ADN contenidos en los índices de referencia de los demás ficheros nacionales de análisis del ADN, para los fines de la persecución de delitos*»[749].

86. En cuanto al nivel de protección de datos, el Capítulo 6 de la Decisión Prüm contiene una serie de disposiciones, que no se limitan a las relativas a los datos genéticos, para proteger la privacidad de los sujetos implicados. En primer lugar, se exige que cada Estado miembro garantice en su Derecho interno «*un nivel de protección de datos equivalente, como mínimo, al que resulta del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y del Protocolo adicional de 8 de noviembre de 2001, y se atendrá a la Recomendación nº R(87) 15, de 17 de septiembre de 1987, del Comité de Ministros del Consejo de Europa a los Estados miembros en relación con la utilización policial de datos de carácter personal, incluso cuando los datos sean objeto de tratamiento no automatizado*»[750].

87. También resulta relevante el artículo 26, que hace referencia al "principio de la finalidad limitada", imponiendo la prohibición de uso de datos para fines distintos de aquellos para los que se le hayan transmitido. Pero, este mismo artículo, tras haber reconocido el principio de la finalidad limitada, prevé que puede derogarse si la legislación nacional del Estado miembro titular del fichero lo permite sin proporcionar ninguna condición adicional a este respecto[751].

---

[749] Si la consulta o la comparación revela una concordancia con alguno de los existentes en sus ficheros de análisis del ADN, será posible que el Estado solicitante obtenga otros datos útiles para la identificación del sujeto. La transmisión de datos debe realizarse a través de los puntos de contacto nacionales, cuya constitución está prevista en el artículo 6 (Punto de contacto nacional y medidas de ejecución) de la Decisión Prüm. El «*sistema que permite saber si el dato buscado está o no («hit/no hit») en la base consultada proporciona una estructura de comparación de perfiles anónimos en la que sólo se intercambian datos personales adicionales una vez encontrada una concordancia; la transmisión y recepción de dichos datos se rige por el derecho interno, incluidas las normas de asistencia judicial. Este sistema asegura una protección adecuada de los datos, siempre que el suministro de datos personales a otro Estado miembro esté supeditado a que este garantice un nivel adecuado de protección de datos*». *Vid*. considerando 18 de la Decisión Prüm.

[750] *Cfr*. artículo 25 (Nivel de protección de datos) de la Decisión Prüm, considerandos 19 y 20. También *vid*. Antonella MARANDOLA (2009: 180 y ss.).

[751] Artículo 26, apartado 1 (Finalidades de la utilización) de la Decisión Prüm: «*El Estado miembro receptor únicamente podrá tratar los datos de carácter personal para los fines para los que se le hayan transmitido con arreglo a la presente Decisión. El tratamiento de los datos para otros fines requerirá la autorización previa del Estado miembro titular del fichero y se hará con sujeción al Derecho interno del Estado miembro receptor. La autorización podrá concederse cuando en el Derecho interno del Estado miembro titular del fichero se admita el tratamiento para los otros fines de que se trate*».

88. Sin embargo, los principales problemas se refieren al ámbito de aplicación de las normas sobre protección de datos personales contenidas en la Decisión Prüm. De hecho, dichas disposiciones se aplican únicamente a los datos transmitidos entre Estados miembros, o puestos a su disposición para ese fin, y no a los tratados exclusivamente a nivel nacional. A este respecto, se señala que la misma situación caracteriza también la siguiente Decisión Marco 2008/977/JAI sobre protección de datos en el denominado antiguo tercer pilar comunitario (cooperación policial y judicial)[752] (*vid*. *supra*). Esta misma situación se mantiene en la nueva Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, articulo 60 (Actos jurídicos de la Unión en vigor)[753].

89. Por tanto, las bases de datos disponibles en virtud de la Decisión Prüm[754] se rigen exclusivamente por la legislación nacional[755], pero el intercambio de datos se rige además por la Decisión, cuya compatibilidad con la nueva Directiva de protección de datos para asuntos policiales y judiciales deberá evaluarse. Los organismos competentes para la

[752] En particular, *vid*. el considerando 20 de la Decisión Prüm: «*Las disposiciones sobre protección de datos que contiene la presente Decisión incluyen también principios de protección de datos que resultaron necesarios por carecerse de una Decisión marco sobre protección de datos en el tercer pilar. Esa Decisión marco deberá aplicarse a todo el ámbito de la cooperación policial y judicial en materia penal con la condición de que su nivel de protección de datos no sea inferior a la protección establecida en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, y su Protocolo adicional de 8 de noviembre de 2001, y tomará en cuenta la Recomendación nº R(87) 15, de 17 de septiembre de 1987, del Comité de Ministros a los Estados miembros, dirigida a regular la utilización de datos de carácter personal en el sector de la policía, también cuando los datos no sean tratados de forma automática*».

[753] Artículo 60 (Actos jurídicos de la Unión en vigor): «*Las disposiciones específicas relativas a la protección de datos personales en actos jurídicos de la Unión que entraron en vigor antes del 6 de mayo de 2016 en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, que regulen el tratamiento entre los Estados miembros y el acceso de autoridades designadas de los Estados miembros a los sistemas de información establecidos con arreglo a lo dispuesto en los Tratados en el ámbito de la presente Directiva no se verán afectadas*».

[754] El enorme potencial de los datos genéticos como herramienta para combatir la delincuencia no puede subestimar los riesgos que su uso implica para los derechos de las personas afectadas. El uso del análisis de ADN, de hecho, implica intrusiones pesadas en su esfera privada, permitiendo el acceso a información sobre características personales muy sensibles, como las relacionadas con el estado de salud. Por lo tanto, es cada vez más urgente encontrar un equilibrio entre el uso de herramientas tecnológicas sin duda muy eficaces en la lucha contra la delincuencia y la protección de la intimidad de los sujetos involucrados. Más detalle, *vid*. Claudia MORINI (2008), «La Convenzione di Prüm sulla cooperazione transfrontaliera specialmente in materia di lotta al terrorismo, al crimine transnazionale e all'immigrazione illegale», en *Studi sull'integrazione europea*, núm. 1, págs. 181-201. Disponible en Internet: http://www.studisullintegrazioneeuropea.eu/Scarico/Rivista%20Studi%200108.pdf [consulta: 19 de julio de 2015]; «Profundización de la cooperación transfronteriza (Decisión Prüm)», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:jl0005#KEYTERMS [consulta: 21 de julio de 2015].

[755] Los Estados deberán garantizar la exactitud y actualidad de dichos datos, y adoptar medidas para rectificar o cancelar los datos incorrectos o los que se hayan transmitido por error. Los datos de carácter personal deberán eliminarse cuando ya no sean necesarios para el fin con que se transmitieron o cuando haya vencido su plazo de conservación según lo dispuesto en la legislación nacional. Artículo 28 (Exactitud, actualidad y duración del almacenamiento de los datos) de la Decisión Prüm. Antonella MARANDOLA (2009: 181-182).

supervisión de dichos flujos de datos son las autoridades nacionales de supervisión de la protección de datos[756].

90. El aumento de la cooperación policial y judicial en materia penal «*debe llevar aparejado el respeto de los derechos fundamentales, en particular el derecho al respeto a la intimidad y a la protección de los datos personales, que debe garantizarse mediante disposiciones especiales de protección de datos adecuadas a las características específicas de las diferentes formas de intercambio de datos. Tales disposiciones de protección de datos deben tener particularmente en cuenta las características propias del acceso transfronterizo en línea a las bases de datos*», estableciendo un sistema que garantice la ejecución de verificaciones *a posteriori*[757].

91. El potencial de los datos genéticos en la lucha con la delincuencia organizada y el terrorismo contrasta con los riesgos de intrusión en la esfera privada de las personas afectadas, sobre todo por el aumento de dichos riesgos derivado del uso de herramientas electrónicas o automatizadas de gestión de la información. También puede haber discriminación o estigmatización de grupos sociales "en riesgo" por el uso de técnicas de perfil racial.

92. La elección de la Decisión Prüm de asignar la creación de bases de datos de ADN sin la concreción de unas normas mínimas relativas a la recogida y tratamiento de dichos datos a nivel nacional resulta criticable por una serie de razones[758]. Entre otras, la falta de unas normas comunes que los Estados miembros tengan que respetar durante todas las fases

[756] Las autoridades pertinentes deben adoptar medidas técnicas y organizativas para proteger los datos personales de su posible destrucción, pérdida, acceso no autorizado, alteración o divulgación. Para poder verificar la licitud del procesamiento de datos personales no automatizado, es preciso registrarlo. Del mismo modo, el procesamiento automatizado de datos personales también requiere un registro. Las autoridades en materia de protección de datos independientes de los países de la UE se encargarán de llevar a cabo las comprobaciones que exige la ley para el procesamiento de datos personales. Artículo 29 (Medidas técnicas y organizativas para garantizar la protección de los datos y su seguridad) y artículo 30 (Documentación y registro; disposiciones especiales relativas a la transmisión automatizada y no automatizada) de la Decisión Prüm. En particular *vid*. Antonella MARANDOLA (2009: 182-184).

[757] Considerando 17 de la Decisión Prüm.

[758] *Cfr*. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la iniciativa del Reino de Bélgica, la República de Bulgaria, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos, la República de Austria, la República de Eslovenia, la República Eslovaca, la República Italiana, la República de Finlandia, la República Portuguesa, Rumanía y el Reino de Suecia con vistas a la adopción de la Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, C 169 de 21.7.2007, págs. 2–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0721(01) [consulta: 28 de julio de 2015].

del tratamiento de datos es probable que dificulte el flujo de información entre las diferentes autoridades nacionales, dadas las diferencias significativas entre las distintas leyes nacionales sobre ficheros nacionales de análisis del ADN. En este sentido, como se ha indicado, es posible derogar el principio de finalidad si la ley del Estado que gestiona la base de datos lo permite.

93. Todo este sistema que se desarrolla dentro del marco de Prüm «*funciona actualmente por debajo de su potencial*», ya que «*no todos los Estados miembros han cumplido sus obligaciones legales en términos de integración de la red en sus propios sistemas*»[759].

94. Sin embargo, como ya se ha señalado anteriormente, para incrementar sustancialmente los niveles actuales de intercambio de información, es necesario seguir fortaleciendo los mecanismos que fomenten la confianza mutua entre las autoridades en materia de seguridad interior, profundizando en los mecanismos existentes y potenciando la estrategia de gestión de la información y el desarrollo de un modelo europeo de intercambio de información seguro y estructurado[760]. Sin embargo, la cuestión es delicada ya que, en lo que respecta a la obtención de datos y el intercambio de información, no sólo se debe garantizar una mayor seguridad para los ciudadanos de los Estados europeos, sino también el respeto de sus derechos fundamentales, entre los que se encuentra, su derecho a la protección de datos y el derecho a la privacidad.

95. En efecto, éste es, sin duda, el aspecto más problemático, ya que el marco de Prüm no ofrece garantías adecuadas en cuanto a la protección de los derechos individuales. La elección hecha por el legislador europeo se encaja en un marco regulador en el que puede apreciarse una cierta tendencia a privilegiar la seguridad y el orden público por encima de la protección de los derechos fundamentales[761]. Una situación complicada, que entra en

[759] La Comisión utilizando «*los poderes que se le han conferido para garantizar el pleno cumplimiento de las obligaciones legales de los Estados miembros, inició un diálogo estructurado ("EU Pilot") con los Estados miembros*» para la plena aplicación del marco de Prüm. En este sentido, la Comisión en 2016 empezó procedimientos de infracciones contra Italia, Croacia, Grecia, Irlanda y Portugal, por no aplicar las Decisiones de Prüm (Decisiones 2008/615/JAI y 2008/616/JAI del Consejo). Francesca GALLI (2016), «UE e cooperazione giudiziaria: se l'Italia non attua Prüm», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/2016/11/ue-e-cooperazione-giudiziaria-se-litalia-non-attua-prum/ [consulta: 26 de agosto de 2017]; COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final.

[760] Antonio M. DÍAZ FERNÁNDEZ (2012: 183).

[761] Un fallo del TEDH que hizo doctrina demuestra que las preocupaciones expresadas no son meramente teóricas. El caso se refiere a Inglaterra, país que tiene la mayor base de datos de ADN del mundo, al menos en proporción a su población. Esto se debe a que, desde 2001, se previó la conservación indefinida de muestras y

conflicto directamente con las disposiciones de la Carta de los Derechos Fundamentales de la Unión Europea, el artículo 6, apartado 1 del TUE y, más concretamente, también el artículo 67, apartado 1 del TFUE que constituye un ELSJ dentro del respeto de los derechos fundamentales.

96. Para concluir este apartado, no puede olvidarse que las Decisiones Prüm son un elemento importante en el marco de la Agenda Europea de Seguridad para el período 2015-2020[762], que establece medidas e instrumentos concretos que se utilizarán en la cooperación para garantizar la seguridad y hacer frente a las amenazas más acuciantes. La Agenda es un memorándum compartido entre la Unión y los Estados miembros, instando a todos los implicados a trabajar juntos para hacer frente, respetando al mismo tiempo la responsabilidad nacional para la defensa de la ley y salvaguardar la seguridad interior, a los desafíos que deben ser abordados con mayor urgencia en la lucha contra el terrorismo, el crimen organizado y los delitos cibernéticos, como áreas interconectadas con fuerte dimensión transfronteriza. El documento destaca una serie de objetivos que se deben alcanzar a realizar, tanto a nivel europeo como nacional, entre los que se encuentra el «*mejor intercambio de información*» entre las autoridades responsable de la seguridad y las agencias del UE; «*mayor cooperación operativa*» entre las autoridades de los distintos Estados miembros; «*formación, financiación, investigación e innovación*» a las acciones relacionadas con la seguridad a nivel de la UE.

perfiles biológicos de ADN de todos los individuos simplemente sospechosos de haber cometido también una categoría de crímenes no graves. La sentencia del TEDH a la que nos referimos es la sentencia *S. and Marper contra Reino Unido* de 2008, en la que el Tribunal sancionó la incompatibilidad de la legislación británica sobre la recopilación y conservación de datos de ADN con el derecho a la intimidad, tal como se menciona en el artículo 8 del CEDH. Más detalles al respecto se pueden encontrar *supra* en la parte relevante la jurisprudencia de este Tribunal y en la doctrina por Gloria GONZÁLEZ FUSTER (2009).

[762] En esta perspectiva, con el objetivo de reforzar la seguridad interior de la UE a la luz de los recientes ataques terroristas en las distintas capitales europeas (París, Copenhague y Bruselas), han llevado a las instituciones europeas a acelerar con respecto a la Agenda Europea de Seguridad para el período 2015-2020 presentada por la Comisión Europea el 28 de abril de 2015, que incluye la lucha contra el terrorismo como una prioridad y es compatible con algunas de las directrices señaladas por los jefes de Estado y de Gobierno en su declaración de 12 de febrero 2015 sobre la lucha contra el terrorismo. Con la Agenda la Comisión Europea ha definido la estrategia de la Unión para hacer frente a las amenazas a la seguridad interna en el período 2015-2020. CONSEJO EUROPEO CONSEJO DE LA UNIÓN EUROPEA - Comunicados de prensa y declaraciones (2015), Reunión informal de los jefes de Estado o de Gobierno Bruselas, 12 de febrero de 2015 - Declaración de los miembros del Consejo Europeo, 12/2/2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/ [consulta: 26 de mayo de 2015]; COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Agenda Europea de Seguridad, COM(2015) 185 final, Estrasburgo, 28/4/2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52015DC0185 [consulta: 26 de mayo de 2015].

97. La Agenda pone de manifiesto que es necesario garantizar «*el pleno cumplimiento de los derechos fundamentales. La seguridad y el respeto de los derechos fundamentales no son objetivos contradictorios, sino objetivos políticos coherentes y complementarios. El enfoque de la Unión se basa en los valores democráticos comunes de nuestras sociedades abiertas, en particular el Estado de Derecho, y debe respetar y promover los derechos fundamentales establecidos en la Carta de los Derechos Fundamentales. Todas las medidas de seguridad deben cumplir los principios de necesidad, proporcionalidad y legalidad, con las salvaguardias adecuadas para garantizar la rendición de cuentas y el recurso judicial*»[763]. Asimismo, se establecen una serie de objetivos, para el que se enumeran las iniciativas ya realizadas y las que se toman a nivel europeo, así como los compromisos a cargo de los Estados miembros.

98. La Comisión Europea hace hincapié en la "necesidad de una mejor cooperación y más eficaz intercambio de información entre las autoridades policiales de los organismos de los Estados miembros de la UE y la interoperabilidad de las bases de datos y sistemas de información". Con este fin, se insta a la rápida ejecución por los Estados miembros de la Directiva relativa a la protección de datos para la policía y las autoridades judiciales penales (adoptada el 14 de abril de 2016) y la conclusión de un acuerdo marco internacional ("Acuerdo marco sobre protección de datos")[764] con el fin de garantizar un elevado nivel de protección de los datos personales que se transfieren entre la UE y los EE.UU. para la prevención, detección, investigación y persecución de las infracciones penales, en particular el terrorismo. Por último, «*la acción de la UE debe centrarse en primer lugar en la plena aplicación de las normas ya vigentes -como el marco de Prüm - y* (…) *la Directiva PNR de la UE, el Reglamento de Europol y la reforma de la protección de datos. Esto ya supondrá un gran paso adelante al implantar un conjunto de instrumentos*

[763] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Agenda Europea de Seguridad. Véase el artículo 6 de la CDFUE y la sentencia del Tribunal de Justicia Europeo, de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12 (*Digital Rights Ireland*), apartado 42. También en conjunto con el artículo 52, apartado 1, de la CDFUE.

[764] El Acuerdo "*Umbrella Agreement*" se firmó el 2 de junio de 2016. El Acuerdo abarca la protección de los datos personales en el contexto de la cooperación policial. El Acuerdo mejora, en particular, los derechos de los ciudadanos de la UE, garantizando la igualdad de tratamiento en comparación con los ciudadanos de los Estados Unidos cuando se trata de recurso judicial delante de los tribunales de Estados Unidos. Vid. EUROPEAN COMMISSION - Statement (2016c), Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting, Amsterdam, 2 June 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-2040_en.htm [consulta: 09 de enero de 2017]. Este Acuerdo será analizado en particular en el Capítulo IV, *infra*.

claro, seguro y bien regulado para dar a las autoridades la información que necesitan, siempre que estas herramientas se exploten plenamente»[765].

99. En consecuencia, la tensión entra la protección de la privacidad y la posibilidad de que se prevea un intercambio de información entre las autoridades europeas en materia de seguridad divide a los Estados europeos, justo cuando sería deseable una posición común y una estrategia común[766]. Es necesario actuar con una mayor cooperación entre los Estados y que no se produzcan divisiones. En ese sentido, y considerando las nuevas y complejas amenazas que acechan a la UE en los últimos años, sería útil la participación plena de los Estados en el marco de Prüm que permitiría alcanzar un mayor nivel de seguridad europea a nivel europeo: permitiría a las autoridades policiales ahorrar tiempo y aumentar la eficiencia en la identificación de sospechosos o de rastros encontrados en el lugar de un crimen; la centralización de los perfiles, en particular, permite una economía de gestión con respecto a la pluralidad de estructuras organizativas en el territorio nacional que caracteriza la situación actual; la cooperación permitiría también un acceso rápido y simplificado a las huellas dactilares y a los perfiles de ADN en las bases de datos de otros países contratantes.

6. Europol: privacidad e intercambio de información policial para la salvaguardia de la seguridad en la UE

100. Como se ha indicado de forma reiterada, la lucha contra el terrorismo, que surge tanto a nivel nacional como internacional, es una cuestión presente de forma permanente en la agenda política dados los actos violentos que se suceden de forma periódica en todo el territorio de la UE (París, Niza, Bruselas, Berlín, Barcelona) que exige un intercambio más sistemático de información y datos, especialmente en el ámbito policial. En la Unión Europea, entre los muchos medios utilizados en la lucha contra el terrorismo, la Agencia Europea de Cooperación Policial, Europol, tiene ciertamente un papel de liderazgo. El intercambio de información entre las fuerzas policiales nacionales de los países miembros

[765] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, COM(2015) 185 final.

[766] La Comisión ha presentado el 18 de octubre de 2017, junto con el undécimo informe sobre la Unión de la Seguridad, una serie de medidas prácticas y operativas para defender mejor a los ciudadanos de la UE contra las amenazas terroristas y conseguir una Europa que proteja a sus ciudadanos. «Unión de la Seguridad: la Comisión presenta nuevas medidas para proteger mejor a los ciudadanos de la UE», en *Diario La Ley*, Wolters Kluwer, 21-11-2017.

de Europol o del Acuerdo de Schengen, son ejemplos de esta nueva justificación para el flujo transfronterizo de datos personales[767].

101. Europol se creó en 1995 con el Convenio Europol[768], con el objetivo de dar apoyo a los Estados miembros en la prevención y lucha contra delitos graves, y comenzó sus actividades en 1999, como estaba previsto en el Título VI del Tratado de Maastricht sobre la cooperación en materia de justicia y asuntos de interior, con especial referencia a la institución de la Oficina Europea de Policía (Europol). El Convenio establece «*unos requisitos mínimos en materia de protección de datos personales que deberán cumplir los Estados miembros que sean parte*» de éste[769].

102. Los Tratados de Ámsterdam, Niza y Lisboa han tenido un impacto sobre el papel de Europol con la ampliación de las tareas y la inclusión de formas de cooperación con otros órganos destinados a operar en la esfera de la política criminal y judicial de la UE. Esto ha motivado que el Convenio Europol de 1995 haya sido modificado por algunos protocolos posteriores, llegando a la adopción, en 2009, de la Decisión del Consejo sobre Europol (en adelante, Decisión Europol)[770], por la que se crea la Oficina Europea de Policía (Europol), que pasó de ser una organización internacional a ser una agencia europea, y en la que se regulan sus aspectos esenciales. Europol tiene como objetivo «*mejorar la cooperación policial entre los Estados miembros para luchar contra el terrorismo, el tráfico ilícito de drogas y demás formas graves de delincuencia organizada internacional*»[771]. Los Estados

[767] Cristian BARBIERI (2017), «Terrorismo: l'arma dello scambio dei dati», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/2017/05/terrorismo-larma-dello-scambio-dei-dati/ [consulta: 28 de agosto de 2017].

[768] Convenio de 26 de julio de 1995, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea la Oficina Europea de Policía, con entrada en vigor el 1 de octubre de 1998. Europol tiene su sede central en La Haya (Holanda). *Vid*. ACTO DEL CONSEJO, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), *Diario Oficial*, C 316 de 27.11.1995, pág. 0001. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995F1127(01) [consulta: 04 de junio de 2015]; «Europol: Oficina Europea de Policía», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l14005b [consulta: 04 de junio de 2015].

[769] Javier ÁLVAREZ HERNANDO (2011: 577).

[770] DECISIÓN DEL CONSEJO, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (2009/371/JAI), *Diario Oficial de la Unión Europea*, L 121 de 15.5.2009, págs. 37–66. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32009D0371 [consulta: 04 de junio de 2015]. Julieta CARMONA BERMEJO (2013), «Instituciones de apoyo a la Cooperación: Red Judicial Europea, Eurojust, Europol, Interpol, Magistrados de Enlace, IberRed», en Miguel CARMONA RUANO, Ignacio U. GONZÁLEZ VEGA, Víctor MORENO CATENA (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 964 y ss.

[771] Artículo 3 (Objetivo) de la Decisión Europol.

miembros cuentan con unidades nacionales que constituyen el vínculo entre Europol y los servicios nacionales competentes en materia de lucha contra la delincuencia[772].

103. Europol tiene personalidad jurídica y su misión es «*apoyar y reforzar la acción de las autoridades competentes de los Estados miembros y su cooperación mutua*» en la prevención y el control de los delitos graves que afectan a «*dos o más Estados miembros, el terrorismo y las formas de delincuencia*» o daño, un interés común objeto de la política de la Unión. Europol es el principal instrumento a nivel europeo para la asistencia a las autoridades de lucha contra el crimen en los Estados miembros de la UE[773].

104. Después de un largo trabajo de negociación[774], con la votación del Parlamento Europeo en segunda lectura, sin ninguna enmienda, se puso fin al proceso legislativo

[772] Sobre la Decisión Europol, véanse la siguiente doctrina: Juan SANTOS VARA (2003), «El desarrollo de las competencias de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, págs. 141-179. ISSN: 1138-4026. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=635314 [consulta: 08 de marzo de 2016]; Patricia ESQUINAS VALVERDE (2010), *Protección de datos personales en la Policía Europea*, Valencia, Tirant lo Blanch, págs. 163; Anselmo DEL MORAL TORRES (2010), «La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal», en *Análisis del Real Instituto Elcano (ARI)*, núm. 50; Andreea MARICA (2012), «El sistema de tratamiento de la información en EUROPOL», en *Institut de Ciències Polítiques i Socials (ICPS)*, WP núm. 309, págs. 30. Disponible en Internet: http://www.icps.cat/archivos/Workingpapers/wp309.pdf?noga=1 [consulta: 10 de marzo de 2016]; Alba BOSCH MOLINÉ (2014), «La dimensión exterior de Europol desde el punto de vista de la protección de datos. El caso del acuerdo TFTP», en *Institute of Audit & IT-Governance (IAITG)*, págs. 33. Disponible en Internet: http://www.iaitg.eu/mediapool/67/671026/data/20140407_abosch_Europol.pdf [consulta: 10 de noviembre de 2016].

[773] Artículo 3 (Objetivo) de la Decisión Europol. Europol intercambia miles de datos cada día, y se ha convertido en un organismo esencial para las autoridades policiales nacionales. Europol se ha convertido hoy en día en la agencia europea que trata el mayor volumen de información dentro de la UE, intercambiando más de 200.000 mensajes en un solo cuatrimestre. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Segundo informe sobre la aplicación de la Estrategia de Seguridad Interior de la UE, COM(2013) 179 final, 10.4.2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52013DC0179 [consulta: 18 de noviembre de 2016].

[774] La Comisión Europea presentó en marzo de 2013, una «*propuesta de Reglamento relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol)*» con los siguientes objetivos: alinear el contenido con los requisitos del Tratado de Lisboa, aumentando su responsabilización, mediante el marco jurídico de Europol y la introducción de un mecanismo de control de sus actividades por parte del Parlamento Europeo junto con los parlamentos nacionales; situar a Europol como eje para el intercambio de información entre las autoridades policiales de los Estados miembros, de modo que pueda apoyar mejor a los Estados miembros e informar mejor la elaboración de políticas de la UE, intensificando el suministro de información de los Estados miembros a Europol; garantizar un sólido régimen de protección de datos aplicable a Europol, en línea con el paquete legislativo sobre protección de datos, en particular en el que el Supervisor Europeo de Protección de Datos de Europol sea plenamente independiente y cooperar con las autoridades de control nacional, actuando de manera eficaz y con poderes suficientes para intervenir; y dotar a Europol de un sistema de gestión de datos flexible y moderno, con la alineación de la gobernanza de las directrices generales aplicables a las agencias europeas. PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) y por el que se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, COM(2013) 173 final, Bruselas, 27.3.2013. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0173_/com_com(2013)0173_es.pdf [consulta: 22 de noviembre de 2016]. Esta propuesta ha sido aprobada de conformidad con el procedimiento legislativo ordinario: «*el Parlamento Europeo y el Consejo determinarán, mediante*

empezado en 2013[775]. Por lo tanto, la Decisión Europol fue derogada y sustituida, a su vez, por el nuevo Reglamento (UE) 2016/794[776] (en adelante, Reglamento Europol), aplicable a partir del 1 de mayo de 2017[777]. El Reglamento Europol adapta Europol a los requisitos del Tratado de Lisboa y mejora su rendición de cuentas ya que, entre otras cosas, garantiza el «*control de las actividades de Europol por el Parlamento Europeo junto con los parlamentos nacionales*»[778]. Se observa que se ha completado sustancialmente el proceso de adopción de la reforma de Europol, con el fin de aplicar plenamente las disposiciones del Tratado que lo conciernen.

105. El nuevo Reglamento basado en el artículo 88 del TFUE, hace más eficiente Europol y "fortifica su régimen de protección de datos, con el fin de brindar el mejor apoyo posible a los esfuerzos de los Estados miembros en la lucha contra la delincuencia". Por tanto, en virtud del artículo 88 del TFUE, la misión de Europol es apoyar y reforzar la acción de la policía y otros servicios policiales de los Estados miembros y su «*cooperación mutua en la prevención y la lucha contra la delincuencia grave que afecte a dos o más Estados miembros, el terrorismo y las formas de delincuencia que lesionen un interés común que sea objeto de una política de la Unión*»[779]. Su estructura, funcionamiento, ámbito de actuación

reglamentos adoptados con arreglo al procedimiento legislativo ordinario, la estructura, el funcionamiento, el ámbito de actuación y las competencias de Europol». *Vid*. *infra*, artículo 88, apartado 2, del TFUE.

[775] El 10 de marzo de, 2016, el Consejo de Justicia y Asuntos de Interior (JAI) adoptó su posición en primera lectura, abriendo el camino para la aprobación definitiva del Reglamento por el pleno del Parlamento Europeo el 11 de mayo de 2016. Con el voto del Parlamento Europa en la segunda lectura, sin enmiendas, se concluyó el proceso legislativo. Vid. SERVIZIO STUDI DEL SENATO (2016a), *Europol ed Eurojust: l'Unione europea e la lotta al terrorismo*, dossier núm. 331, pág. 20. Disponible en Internet: https://www.senato.it/service/PDF/PDFServer/BGT/00977222.pdf [consulta: 05 de diciembre de 2016].

[776] REGLAMENTO (UE) 2016/794 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, *Diario Oficial de la Unión Europea*, L 135/53 de 24.5.2016, págs. 53–114. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0794 [consulta: 10 de diciembre de 2016].

[777] El Reglamento entró en vigor 20 días después de su publicación en el Diario Oficial de la UE y ha tenido efecto desde el 1 de mayo de 2017. Artículo 77 (Entrada en vigor y aplicación) del Reglamento Europol.

[778] *Vid*. Covadonga FERRER MARTÍN DE VIDALES (2008), «Los parlamentos nacionales en la Unión Europea tras el Tratado de Lisboa», en *Jean Monnet/Robert Schuman Paper Series*, vol. 8, núm. 16, págs. 33. Disponible en Internet: http://aei.pitt.edu/8907/1/deVidalesEUparliamentosLong08edi.pdf [consulta: 08 de marzo de 2016]; Daniele CODUTI (2015), «Europol e ruolo dei parlamenti (nazionali ed europeo): quali prospettive dopo il Trattato di Lisbona?», en *Diritto Pubblico Europeo Rassegna online*, luglio, págs. 23. ISSN: 2421-0528. Disponible en Internet: http://www.edizioniesi.it/dperonline/data/uploads/articoli/coduti-europol.pdf [consulta: 10 de marzo de 2016].

[779] Artículo 88 (antiguo artículo 30 TUE): «*1. La función de Europol es apoyar y reforzar la actuación de las autoridades policiales y de los demás servicios con funciones coercitivas de los Estados miembros, así como su colaboración mutua en la prevención de la delincuencia grave que afecte a dos o más Estados miembros, del terrorismo y de las formas de delincuencia que lesionen un interés común que sea objeto de una política de la Unión, así como en la lucha en contra de ellos. 2. El Parlamento Europeo y el Consejo determinarán, mediante reglamentos adoptados con arreglo al procedimiento legislativo ordinario, la estructura, el funcionamiento, el ámbito de actuación y las competencias de Europol. Estas competencias podrán incluir: a) la recogida, almacenamiento, tratamiento, análisis e intercambio de la información, en particular la transmitida por las autoridades de los Estados miembros o de terceros países o terceras instancias; b) la*

y competencias se regirán por un reglamento adoptado por el procedimiento legislativo ordinario. Se señala que, entre sus competencias, expresamente, se mencionan la "recogida", "almacenamiento", "tratamiento", "análisis" e "intercambio de la información, en particular la transmitida por las autoridades de los Estados miembros o de terceros países o terceras instancias" (apartado 2). El artículo 88 del TFUE también requiere que los colegisladores establezcan los procedimientos para el control de sus actividades por parte del Parlamento Europeo, en los parlamentos nacionales.

106. A continuación, se trata de identificar brevemente sus principales características, atendiendo a los aspectos más problemáticos en relación con el control democrático y la protección de la privacidad, con el fin de evaluar los posibles desarrollos futuros, considerando la sustitución de la Decisión Europol[780] con el nuevo Reglamento Europol adoptado con arreglo al procedimiento legislativo ordinario. Ya desde la naturaleza jurídica del acto se pueden ver los primeros cambios fundamentales: ya no es una decisión del Consejo, sino que la intervención del Parlamento Europeo hace este instrumento (el Reglamento) más democrático y sobre todo acordada no sólo de manera intergubernamental, sino también entre las fuerzas políticas de los distintos Estados miembros de la Unión.

107. Según el artículo 3, apartado 1 del Reglamento Europol, la Agencia tiene el objetivo de apoyar y reforzar la «*actuación de las autoridades competentes de los Estados miembros y su cooperación mutua en la prevención y la lucha contra la delincuencia grave que afecte a dos o más Estados miembros, el terrorismo y las formas de delincuencia que afectar a un interés común*» que sea objeto de una política de la Unión[781].

---

coordinación, organización y realización de investigaciones y actividades operativas, llevadas a cabo conjuntamente con las autoridades competentes de los Estados miembros o en el marco de equipos conjuntos de investigación, en su caso en colaboración con Eurojust. En dichos reglamentos se fijará asimismo el procedimiento de control de las actividades de Europol por el Parlamento Europeo, control en el que participarán los Parlamentos nacionales. 3. Cualquier actividad operativa de Europol deberá llevarse a cabo en contacto y de acuerdo con las autoridades de los Estados miembros cuyo territorio resulte afectado. La aplicación de medidas coercitivas corresponderá exclusivamente a las autoridades nacionales competentes». *Vid*. *supra* también el apartado del Capítulo II sobre el artículo 88 del TFUE.

[780] La Decisión tenía fundamento jurídico en el Tratado de la Unión Europea y, en particular, su artículo 30, apartado 1, letra b), su artículo 30, apartado 2, y su artículo 34, apartado 2, letra c).

[781] El artículo 3 (Objetivos), apartado 1 del Reglamento Europol, hace referencia a la lista de formas de delincuencia contenidas en el anexo I de la misma norma. *Vid*. Anexo I - Lista de formas de delincuencia a las que hace referencia el artículo 3, apartado 1: «*terrorismo, delincuencia organizada, tráfico de estupefacientes, actividades de blanqueo de capitales, delitos relacionados con materiales nucleares o sustancias radiactivas, tráfico de inmigrantes, trata de seres humanos, delincuencia relacionada con el tráfico de vehículos robados, homicidio voluntario y agresión con lesiones graves, tráfico ilícito de órganos y tejidos humanos, secuestro, retención ilegal y toma de rehenes, racismo y xenofobia, robo y hurto con agravantes, tráfico ilícito de bienes culturales, incluidas las antigüedades y obras de arte, fraude y estafa, delitos contra los intereses financieros de la Unión, operaciones con información privilegiada y manipulación del mercado, chantaje y extorsión, violación de derechos de propiedad industrial y falsificación de mercancías, falsificación de documentos*

108. Con la nueva Agencia se pretende proporcionar un apoyo más eficaz a los Estados miembros para luchar contra el terrorismo, la delincuencia informática y otros delitos graves, y responder más rápidamente a las amenazas, gracias a las nuevas reglas de *governance* aprobadas por el Parlamento Europeo. Asimismo, el Reglamento Europol convierte a la Agencia en un centro de información en materia delictiva único para las fuerzas y cuerpos de seguridad de la UE, consolidándose como la principal agencia de seguridad interior de la Unión, y al mismo tiempo ofrece unas mayores garantías de protección de los datos[782]. Las nuevas normas de tratamiento de datos permiten a Europol identificar rápidamente tendencias y modelos en todos los ámbitos de delincuencia y crear informes más completos y relevantes para apoyar a las fuerzas y cuerpos de seguridad de los países de la UE.

109. Las principales actividades de Europol se centran en "mejorar el intercambio de información entre las autoridades policiales, potenciando la eficacia de la cooperación policial europea"[783]. Europol es responsable en situaciones en las que los países de la UE

administrativos y tráfico de documentos administrativos falsos, falsificación de moneda, falsificación de medios de pago, delito informático, corrupción, tráfico ilícito de armas, municiones y explosivos, tráfico ilícito de especies animales protegidas, tráfico ilícito de especies y variedades vegetales protegidas, delitos contra el medio ambiente, incluida la contaminación procedente de buques, tráfico ilícito de sustancias hormonales y otros factores de crecimiento, abusos sexuales y explotación sexual, incluido el material sobre abuso de menores y la captación de menores con fines sexuales, genocidio, crímenes de lesa humanidad y crímenes de guerra».

[782] La adopción del Reglamento Europol tuvo lugar sólo 14 días después de la aprobación de la Directiva Europea de Protección de Datos en el ámbito policial o judicial (27 de abril de 2016). La Directiva, aunque excluye las transferencias de datos de Europol de su alcance jurídico, tiene un claro impacto directo sobre el Reglamento de Europol. En este sentido, el considerando 40 del Reglamento Europol resalta la importancia de alinear ambos textos jurídicos: «*Las normas de protección de datos de Europol deben reforzarse y apoyarse en los principios en los que se basa el Reglamento (CE) n. 45/2001 a fin de garantizar un alto nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales. Como la Declaración n. 21 relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial adjunta al TUE y al TFUE reconoce la especificidad del tratamiento de los datos personales en el contexto policial, las normas de protección de datos de Europol deben ser autónomas y al mismo tiempo coherentes con otros instrumentos pertinentes en materia de protección de datos aplicables en el ámbito de la cooperación policial en la Unión. Dichos instrumentos incluyen, en particular, la Directiva (UE) 2016/680 del Parlamento Europeo y de del Consejo, así como el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Recomendación n. R(87) 15*».

[783] En los últimos años, Europol ha incrementado su cooperación con las autoridades policiales de la UE y los terceros países, entre otras cosas mediante la firma de acuerdos bilaterales con Países fuera de la Unión Europea y organizaciones internacionales. Europol trabaja con organismos y agencias de la UE, entre ellos: Eurojust, Oficina Europea de Lucha contra el Fraude (*OLAF*), Banco Central Europeo (BCE), Comisión Europea, Agencia de la Unión Europea para la Formación Policial (*CEPOL*), Frontex, Agencia de Seguridad de las Redes y de la Información de la Unión Europea (*ENISA*), Interpol, etc. Europol realiza una evaluación de la amenaza que representa la delincuencia grave y organizada (*SOCTA* - "*Serious and Organised Crime Threat Assessment*") y elabora un informe sobre la situación y las tendencias del terrorismo en la Unión Europea (*TE-SAT* - "*The European Union Terrorism Situation and Trend Report*"). En particular: en 2013, en la sede de Europol en La Haya se creó el Centro Europeo de Ciberdelincuencia de Europol (*EC3*), responsable, entre otras cosas, de evaluar la amenaza del crimen organizado en Internet; después de los ataques terroristas en París y Copenhague a principios de 2015, se estableció una unidad para luchar contra la propaganda terrorista en línea; y siempre como resultado de los ataques de noviembre de 2015, en París, el Consejo amplió el mandato de Europol contra el terrorismo con el lanzamiento, como dicho, el 1 de enero de 2016, del nuevo Centro

necesitan apoyo para abordar la delincuencia, el terrorismo y otras formas de delincuencia transfronteriza que afectan los intereses de la UE[784].

110. Para alcanzar sus objetivos, Europol desempeña las siguientes funciones: «*recoger, almacenar, tratar, analizar e intercambiar información*»; comunicar a los países de la UE las relaciones entre los actos delictivos que les afecten; asistir a los países de la UE en las investigaciones y proporcionar apoyo en materia de análisis e información; coordinar, organizar y aplicar investigaciones y operaciones para apoyar o reforzar las acciones de los las fuerzas y cuerpos de seguridad de los países de la UE; solicitar a los Países de la UE que inicien, realicen o coordinen investigaciones en casos específicos y sugerir la creación de equipos conjuntos de investigación; apoyar a los países de la UE en materia de prevención y lucha contra formas de delincuencia facilitadas, fomentadas o cometidas a través de internet; redactar evaluaciones de amenazas y otros informes. En particular, el Reglamento fortalece el mandato de Europol para garantizar la plena operatividad frente al aumento de la delincuencia transfronteriza y las amenazas terroristas[785.]

111. El texto aprobado introduce las disposiciones necesarias para el funcionamiento de la unidad de operaciones a través de Internet, que no estaba previstas en la propuesta de la Comisión, y asigna a Europol la tarea de apoyar los Estados miembros "para prevenir y combatir las formas de delincuencia que hayan sido facilitadas, fomentadas o cometidas a través de Internet"[786]. Europol, por lo tanto, tiene esencialmente una función de inteligencia

Europeo Contra el Terrorismo (*ECTC*), se asignan expertos antiterroristas de los Estados miembros con el fin de aumentar la capacidad de investigación internacional; el 7 de abril de 2016, la Agencia Federal de Investigaciones de EE.UU. *Federal Bureau of Investigation* (FBI) y Europol firmaron un acuerdo para intensificar las acciones conjuntas para luchar contra los combatientes terroristas extranjeros. En virtud de este acuerdo, el FBI puede participar en el intercambio de información coordinado por la red de puntos focales de Europol *Travellers*, principales herramientas de Europol para combatir a los terroristas extranjeros y las redes terroristas conexas

[784] Alberto PÉREZ DÍAZ-HEREDERO (2016).

[785] *Vid*. *amplius* artículo 4 (Funciones) del Reglamento Europol. Con este artículo se manifiesta la alineación del Reglamento Europol con el Tratado de Lisboa el cual describe las mismas tareas de coordinación que las que se encuentran en el artículo 88 del TFUE. En particular, será más fácil para Europol instituir unidades especializadas para responder de inmediato a las amenazas emergentes. Las reglas incluirán también orientaciones claras sobre las tareas de los centros existentes como el Centro Europeo de Lucha contra la Ciberdelincuencia. Artículo 4, apartado 1, letra l), Reglamento Europol.

[786] Artículo 4, apartado 1, letra m) «*respaldar las acciones de los Estados miembros para prevenir y combatir las formas de delincuencia enumeradas en el anexo I que hayan sido facilitadas, fomentadas o cometidas a través de internet, incluyendo, en cooperación con los Estados miembros, la notificación de contenidos de internet a través de los cuales se facilitan, fomentan o cometen estas formas de delitos, a los proveedores de servicios en línea interesados para que examinen de manera voluntaria la compatibilidad de esos contenidos de internet con sus propias condiciones contractuales*». El texto adoptado introduce las disposiciones necesarias para el funcionamiento de la Unidad de notificación de contenidos de internet (*Internet Referral Unit - IRU*), no mencionada en la propuesta de la Comisión, y asigna a Europol la tarea de apoyar las acciones de los Estados miembros para prevenir y combatir las formas de delincuencia que se facilitan, fomentan o

en la lucha contra las formas más graves de delincuencia que afecten a dos o más Estados miembros[787], sin la facultad de adoptar medidas coercitivas.

112. Además, se especifica que, para «*mejorar su eficacia a la hora de facilitar análisis criminales exactos a las autoridades competentes de los Estados miembros, Europol debe utilizar las nuevas tecnologías para tratar los datos*». Por consiguiente, «*es preciso estructurar las bases de datos de Europol de tal modo que Europol pueda elegir la estructura informática más eficiente. Asimismo es preciso que Europol pueda actuar como proveedor de servicios, en particular ofreciendo una red segura para el intercambio de datos, como la Aplicación de la Red de Intercambio Seguro de Información (SIENA)*», cuyo objetivo es facilitar el intercambio de información entre los Estados miembros, Europol, otros organismos de la Unión, países terceros y organizaciones internacionales[788]. A fin de "garantizar un alto nivel de protección de datos, deben establecerse la finalidad de las operaciones de tratamiento y los derechos de acceso, así como salvaguardias adicionales

cometen a través de Internet. *Cfr*. *infra* el artículo 26, apartado 5, letra c) del Reglamento Europol en esta misma investigación. La Agenda de Seguridad Europea ha impulsado la introducción de la *IRU* como consecuencia de los atentados terroristas de París y Copenhague en los primeros meses de 2015. El Consejo de Justicia y Asuntos de Interior ha encomendado a Europol a crear una unidad de informes en Internet para combatir la propaganda terrorista en línea y otras actividades extremistas. La nueva unidad inició su actividad el 1 de julio de 2015. La propia Comisión considera que la *IRU* es de vital importancia en el actual contexto de seguridad. Vid. «Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda», en *Press Release Europol*, 01 July 2015. Disponible en Internet: https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda [consulta: 11 de julio de 2017].

[787] El artículo 4, apartado 1 letra c) del Reglamento Europol, establece que Europol desempeñará, entre sus funciones «*coordinar, organizar y ejecutar cualesquiera actuaciones de investigación y operativas para respaldar y reforzar las actuaciones que lleven a cabo las autoridades competentes de los Estados miembros*». Por ello, la Autoridad Común de Control de Europol (ACC) sugirió antes de que se aprobara el Reglamento que se añadieran reglas específicas para que se pudiera comprender mejor la nueva distribución de competencias entre Europol y las autoridades policiales de los Estados miembros durante una investigación criminal. Cristina BLASI CASAGRAN (2016a), «El Reglamento Europeo de Europol: Un nuevo marco jurídico para el intercambio de datos policiales en la UE», en *Revista General de Derecho Europeo*, núm. 40, pág. 205. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5692787 [consulta: 20 de julio de 2017].

[788] Según el considerando 24 del Reglamento Europol. Para el intercambio seguro y rápido de información, Europol ha creado un sistema *ad hoc*, denominado *Secure Information Exchange Network Application* (*SIENA*), mientras que para el manejo y tratamiento de las informaciones recibidas se vale de un sistema informatizado que consta de dos subsistemas: el Sistema de información de Europol y Ficheros de trabajo de análisis. Es usada actualmente por más de 300 autoridades nacionales con el fin de intercambiar información de carácter penal, e intercambia más de 400.000 mensajes operativos al año. Europol usa *SIENA* desde el año 2009 con la finalidad de conectar la agencia en una estructura con garantías adecuadas de seguridad y encriptación. *SIENA* es el principal método de comunicación entre las unidades nacionales de Europol y Europol, pero recientemente también se ha utilizado para intercambiar información con terceros estados, oficiales de enlace de los Estados miembros, personal de Europol y otras autoridades competentes. *Vid*. «Secure Information Exchange Network Application (Siena)», en *europol.europa.eu*. Disponible en Internet: https://www.europol.europa.eu/content/page/siena-1849 [consulta: 22 de julio de 2017].

específicas"[789]. En particular, al tratar los datos personales «*deben respetarse los principios de necesidad y proporcionalidad*»[790].

113. El artículo 6 del nuevo Reglamento prevé la posibilidad de que Europol inicie una investigación propia ("*motu proprio*"), proponiendo a «*las autoridades competentes de los Estados miembros interesados, a través de sus unidades nacionales, que inicien, realicen o coordinen dicha investigación penal*»[791]. Uno de los principales límites de Europol en el pasado era precisamente la falta de autonomía en la acción.

114. Como ya se ha adelantado, el contacto entre Europol y la autoridad competente de un país de la UE se realiza a través de una unidad nacional designada[792]. La «*unidad nacional*» "será el único órgano de enlace entre Europol y las autoridades competentes de los Estados miembros". No obstante, de acuerdo con las condiciones establecidas por el país de la UE en cuestión, los países de la UE pueden permitir el contacto directo con sus autoridades nacionales[793]. Los Estados miembros, a través de su unidad nacional o una autoridad competente, «*suministrarán a Europol la información necesaria para que pueda cumplir sus objetivos*»; «*garantizarán una comunicación y cooperación eficaces con Europol de todas las autoridades competentes pertinentes*»; «*propiciarán el conocimiento de las actividades de Europol*»; y «*garantizarán el cumplimiento del Derecho nacional al*

[789] Parece complicado que se instaure *SIENA* como herramienta de comunicación generalizada dentro de la UE cuando nunca ni el nuevo Reglamento ni la anterior Decisión del Consejo han incorporado ninguna cláusula al respecto. La única excepción es el considerando 26 del Reglamento Europol que es, sin embargo, superficial y azaroso. La falta de disposiciones sobre *SIENA* en el Reglamento se concibe pues como una oportunidad fallida de armonización del alto número de canales existentes hoy en día para intercambiar información en el ámbito de la seguridad.

[790] El considerando 26 del Reglamento Europol destaca: «*Con el fin de respetar la propiedad de los datos y la protección de los datos personales, los Estados miembros, los organismos de la Unión, los países terceros y las organizaciones internacionales deben poder determinar la finalidad o finalidades para las cuales Europol puede tratar los datos que facilitan y restringir los derechos de acceso. La limitación de la finalidad es un principio fundamental del tratamiento de datos personales; en particular, contribuye a la transparencia, la seguridad jurídica y la previsibilidad, y reviste especial importancia en el ámbito de la cooperación policial, en el que los interesados no suelen estar al tanto de la recogida y del tratamiento de sus datos personales, y en el que el uso de datos personales puede repercutir de forma muy significativa en las vidas y libertades de las personas físicas*».

[791] Artículo 6 (Solicitudes cursadas por Europol para la apertura de una investigación penal) del Reglamento Europol.

[792] Artículo 7 (Unidades nacionales de Europol), apartado 2, del Reglamento Europol. El artículo en comentario establece las condiciones bajo las cuales los Estados miembros deben cooperar con Europol. Este artículo muestra grandes cambios respecto a la ley anterior. Principalmente establece una obligación para las autoridades policiales de los Estados miembros de proporcionar a Europol información de carácter penal, cuando la anterior Decisión del Consejo no consagraba dicha obligación. Además, la ley anterior no permitía a Europol acceder a las bases de datos de las autoridades policiales nacionales. Por lo tanto, con el nuevo Reglamento los Estados miembros tienen la obligación de informar a Europol sobre todos los intercambios de datos bilaterales y multilaterales que recaigan dentro del alcance competencial de la agencia. Cristina BLASI CASAGRAN (2016a: 206-207).

[793] Artículo 7, apartado 5, del Reglamento Europol.

proporcionar información a Europol». Con respecto al mantenimiento del orden público y la salvaguardia de la seguridad interior, los Estados miembros no tendrán la obligación de transmitir información si: «*a) fuese contrario a los intereses fundamentales de seguridad del Estado miembro de que se trate; b) comprometiese el resultado de una investigación en curso o la seguridad de una persona, o c) revelase información referida a organizaciones o actividades específicas de inteligencia en materia de seguridad nacional*»[794].

115. Tal y como se ha mencionado anteriormente, en la medida necesaria para alcanzar sus objetivos, Europol podrá tratar información, incluyendo datos de carácter personal[795]. El Capítulo IV (Tratamiento de la información) del Reglamento, por tanto, establece que, a los fines de la prevención y la lucha contra la delincuencia grave en el ámbito de sus objetivos, Europol podrá tratar «*la información que le haya sido facilitada por: los Estados miembros* (…)*; b) organismos de la Unión, países terceros y organizaciones internacionales* (…)*; c) por entidades privadas y particulares* (…)*. Europol podrá extraer y tratar directamente información, incluidos datos personales, procedentes de fuentes públicamente disponibles, en particular internet y datos públicos*»[796].

116. Se distingue cuatro finalidades distintas para el tratamiento de datos en Europol (artículo 18, apartado 2 - Fines de las actividades de tratamiento de la información): «*a) controles cruzados destinados a identificar conexiones u otras relaciones pertinentes entre datos relacionados con: i) las personas que sean sospechosas de haber cometido o de haber participado en un delito penal que sea competencia de Europol o que hayan sido condenadas por tal delito, ii) personas respecto de las cuales existan indicios concretos o motivos razonables para pensar que cometerán delitos penales que son competencia de Europol; b) análisis estratégicos o temáticos; c) análisis operativos; d) facilitar el intercambio de información entre los Estados miembros, Europol, otros organismos de la Unión, países terceros y organizaciones internacionales. El acceso se concede sólo a personal debidamente autorizado de Europol y en la medida necesaria y proporcionada para el cumplimiento de sus funciones*».

[794] Artículo 7, apartados 6 y 7, del Reglamento Europol.
[795] La Decisión del Consejo de 2009 contenía disposiciones obligatorias, que permitió a Europol analizar información dentro de los archivos individuales de trabajo para fines de análisis. El Consejo considera que Europol ha sido hasta ahora incapaz de análisis cruzados entre los archivos y localizar, por ejemplo, enlaces o posibles vínculos entre el crimen organizado y el terrorismo. La Decisión Europol permitió introducir datos en el sistema de información de Europol sobre personas que han cometido o se sospeche que planifican un delito que sea competencia de Europol; estos datos pudieron estar directamente relacionados con la persona (nombre, nacionalidad, números de seguridad social, *etc*.) y con el delito.
[796] Artículo 17 (Fuentes de información) del Reglamento Europol.

117. En las conexiones entre datos, los análisis estratégicos, y el intercambio de datos permiten a los Estados miembros buscar toda la información necesaria que ha sido almacenada en Europol, aunque en el caso de análisis operativos se requiere una mayor protección de los datos. En efecto, el artículo 18 apartado 3, dispone que, en el tratamiento de los datos mediante proyectos de análisis operativos, se deben aplicar garantías específicas tales como «*el objetivo específico, las categorías de datos personales y las categorías de interesados, los participantes, la duración de la conservación y condiciones de acceso, transferencia y uso de los datos* (…)». "El tratamiento posterior de los datos personales sólo se permite en la medida en que ello sea necesario y proporcionado". También se establece que el «*Consejo de Administración, tras haber consultado al SEPD adoptará, según proceda, directrices que concreten más detalladamente los procedimientos de tratamiento de la información* (…)» por parte de Europol (apartado 7).

118. El nuevo sistema debería representar, por el contrario, un entorno de procesamiento de datos diferente que refleje una gestión integrada de datos desde una perspectiva Europol (*Integrated Data Management Concept - IDMC*) y sea compatible con la estructura actual del Sistema de Información de Europol[797].

119. Los Estados miembros, de conformidad con su legislación nacional y «*sin perjuicio del ejercicio por parte de los Estados miembros de sus responsabilidades con respecto al mantenimiento del orden público y la salvaguardia de la seguridad interior*»[798], tienen acceso y pueden consultar toda la información facilitada a los fines del artículo 18, apartado 2, letras a) y b) (*vid*. *supra*). Todo ello «*sin perjuicio*» de los derechos de los Estados miembros, organismos de la Unión, países terceros y organizaciones internaciones. También a los Estados miembros se les reconoce acceso indirecto a dichos datos, sobre la

[797] El artículo 18 ha sido criticado por la poca claridad de cómo Europol va a implementar dicho sistema de tratamiento de datos. A este respecto Cristina BLASI CASAGRAN (2016a: 213) apunta: «*Parece que la idea bajo el Artículo 18 es crear un gran SIE con un único banco de datos compuesto de distintos niveles de tratamiento según la categoría de datos. La finalidad detrás de este cambio no es otra que aumentar la protección de los datos personales estableciendo criterios estrictos para el cumplimiento del principio de limitación de finalidad. Sin embargo, no se da ninguna explicación concreta de cómo se logrará crear este nuevo sistema en la práctica. Tal vez se podría implementar el sistema del Artículo 18 adoptando previamente una evaluación de impacto sobre la privacidad en la que se explicaran la finalidad, necesidad y proporcionalidad antes de abrir un archivo de inclusión de datos*». De hecho, tanto el SEPD como la ACC sugirieron llevar a cabo una evaluación de impacto en protección de datos antes de aprobar el nuevo Reglamento de Europol. Una de las preocupaciones que expresaron estos organismos es que los principios de necesidad y limitación de finalidad no deberían depender de una estructura tecnológica como la que se propone en el artículo 18. Por lo tanto, las evaluaciones de impacto podrían ser una solución a este procedimiento ambiguo, excepto cuando debido a la urgencia no fuera posible demorar la operación para la obtención de datos personales. SERVIZIO STUDI DEL SENATO (2016a: 24).

[798] Artículo 7, apartado 7, del Reglamento Europol.

base de un sistema de respuesta positiva o negativa («*hit/no-hit*»), y siempre que haya una investigación penal en curso[799]. Siempre de conformidad con la legislación nacional, el artículo 20 dispone normas de acceso de los Estados miembros y del personal de Europol a la información almacenada por Europol: «*los Estados miembros tendrán acceso a la información* (…) *y la tratarán ulteriormente solo a efectos de prevenir y combatir: a) formas de delincuencia para las que Europol sea competente, y b) otras formas de delincuencia grave, según se recoge en la Decisión Marco 2002/584/JAI del Consejo*»[800]; el personal de Europol debidamente habilitado tendrá acceso a la información procesada por Europol «*en la medida necesaria para el ejercicio de sus funciones*»[801] y sin exclusión sobre las obligaciones de discreción y confidencialidad y sobre la protección de la información sensible no clasificada[802].

120. Europol puede «*establecer y mantener relaciones de cooperación con los organismos de la Unión de conformidad con los objetivos de dichos organismos, las autoridades de Países terceros, organizaciones internacionales y entidades privadas*»[803]. La Unión Europea ha concedido a Europol acceso a las principales bases de datos centrales, pero la Agencia aún no ha aprovechado plenamente esta oportunidad. Al hilo del tema, a Europol ha sido reconocida la posibilidad de acceder al Sistema de Información de Schengen (SIS II). "La Agencia tiene derecho de acceso y búsqueda directa en los datos introducidos en el SIS para fines de detención, controles discretos y específicos y de la incautación de bienes". Europol ha encaminado los trabajos en la aplicación de las conclusiones del Consejo JAI de 20 de noviembre de 2015, en materia de lucha antiterrorista, para que pueda comprobar sistemáticamente las bases de datos de Europol y el SIS II[804].

---

[799] Artículo 20 (Acceso de los Estados miembros y del personal de Europol a la información conservada por Europol), apartados 1 y 2 del Reglamento Europol. Este sistema primero examinará si la información delictiva que se ha introduce coincide con alguno de los datos almacenados en la base de datos de Europol, y sólo si la respuesta es positiva, el solicitante podrá pedir más información al respecto. De hecho, el mecanismo de respuesta positiva/negativa se ha consolidado desde hace muchos años en Europol y es una medida que claramente asegura una gran protección de datos, mucho mayor que en la mayoría de los sistemas de búsqueda a nivel nacional.

[800] DECISIÓN MARCO 2002/584/JAI DEL CONSEJO, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, *Diario Oficial de la Unión Europea*, L 190 de 18.07.2002, págs. 0001 – 0020.

[801] Artículo 20 (Acceso de los Estados miembros y del personal de Europol a la información conservada por Europol), apartados 3 y 4, del Reglamento Europol.

[802] Artículo 67 (Normas en materia de protección de la información sensible no clasificada y clasificada) del Reglamento Europol.

[803] Artículo 23 (Disposiciones comunes) del Reglamento Europol.

[804] CONSEJO DE LA UNIÓN EUROPEA (2016), Hoja de ruta para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior, 9368/1/16, Bruselas, 6 de junio de 2016, pág. 24; CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015d). La conexión de Europol con el SIS II se inició el 10 de diciembre de 2014.

121. En casos específicos, desde septiembre de 2013, Europol también puede solicitar el acceso a los datos almacenados en el Sistema de Información de Visados (VIS) para la prevención, detección e investigación de delitos de terrorismo y otros delitos graves. Estas consultas deben llevarse a cabo a través de puntos de acceso centrales de los países participantes y de Europol, garantizando la verificación de las solicitudes y asegurando el cumplimiento de la Decisión 2008/633/JAI. También, desde julio de 2015, la base jurídica de Eurodac permite el acceso de Europol[805].

122. Europol dispone de todas las medidas apropiadas para permitir que Eurojust y la *OLAF*[806], en el marco de sus respectivos mandatos., «*tengan acceso indirecto*», sobre la base de un sistema de «*respuesta positiva o negativa*» («*hit/no hit*»), «*a la información facilitada*», sin perjuicio de las restricciones establecidas por los Estados miembros, organismos de la Unión, países terceros u organizaciones internacionales que proporcionaron la información en cuestión[807]. Europol y Eurojust pueden concluir un acuerdo de trabajo que garantice, recíprocamente y dentro del marco de sus respectivos mandatos, «*la posibilidad de acceso a, y búsqueda de, toda la información facilitada,* (…) *y la posibilidad de consultar dicha información, sin perjuicio del derecho de los Estados miembros, organismos de la Unión, países terceros y organizaciones internacionales a indicar restricciones al acceso y la utilización de dichos datos, de conformidad con las garantías de protección de datos establecidas en el presente Reglamento*»[808]. Además, notificará "sin demora" a un Estado miembro cualquier información que le concierna[809].

123. Con la nueva Directiva *PNR* de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (*PNR*) para la prevención, detección, investigación y

[805] CONSEJO DE LA UNIÓN EUROPEA (2016).
[806] Considerando 28 del Reglamento Europol: «*Para mejorar la cooperación operativa entre las agencias y, en particular, para establecer vínculos entre los datos ya en posesión de las diferentes agencias, Europol debe permitir a Eurojust y a la Oficina Europea de Lucha contra el Fraude (OLAF) el acceso mediante un sistema de respuesta positiva o negativa a los datos disponibles en Europol. Europol y Eurojust deben tener la facultad de celebrar un acuerdo de trabajo que garantice de manera recíproca, en el marco de sus respectivos mandatos, la posibilidad de acceder y efectuar búsquedas con respecto a toda la información que se haya facilitado a efectos de verificación cruzada, y la posibilidad de efectuar búsquedas, con arreglo a las salvaguardias y garantías específicas en materia de protección de datos estipuladas en el presente del Reglamento. Cualquier acceso a datos disponibles de Europol se limitaría por medios técnicos a la información que corresponda a los mandatos respectivos de dichos organismos de la Unión*».
[807] En caso de una respuesta positiva, Europol iniciará el procedimiento para que la información que generó la respuesta positiva se pueda compartir, de acuerdo con la decisión del proveedor de información a Europol, y sólo en la medida en que los datos que generaron la respuesta sean necesarios para la realización de las tareas de Eurojust o de la *OLAF*.
[808] *Vid*. artículo 21 (Acceso de Eurojust y de la *OLAF* a la información conservada por Europol), apartados 1 y 2, del Reglamento Europol.
[809] Artículo 22 (Obligación de notificación a los Estados miembros) del Reglamento Europol.

enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, se exige a los Estados miembros el intercambio de datos *PNR* que reciben, entre ellos y con Europol, cuando se considere necesario para la prevención, detección, investigación y enjuiciamiento de delitos terroristas o delitos graves[810]. Este intercambio de datos *PNR* debe estar sujeto a las normas relativas a la cooperación policial y judicial y no debe perjudicar al alto nivel de protección de la privacidad y los datos personales proporcionados por la CDFUE, el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio n. 108) y el CEDH. La seguridad del intercambio de información relativa a los datos *PNR* también estará garantizada por uno de los canales existentes de cooperación entre las autoridades competentes de los Estados miembros y, en particular, con Europol a través de la aplicación de la red para el intercambio de información protegida (*SIENA*).

124. Para garantizar la limitación de la finalidad[811], Europol tiene reconocida la capacidad, bajo ciertas condiciones, de «*transferir directamente datos personales a un organismo de la Unión en la medida en que la transferencia sea necesaria para prevenir y combatir los delitos*» declarados en los objetivos de Europol[812]. Con este fin, en el caso de la transferencia de datos personales, es necesario garantizar que el receptor garantice que utilizará los datos o procederá a su posterior transferencia a una autoridad competente de un tercer país únicamente para los fines para los que fueron transferidos inicialmente. La ulterior transferencia de datos debería realizarse de conformidad con el presente Reglamento. En este ámbito, el Reglamento consolida el papel de la Comisión, en la evaluación de los acuerdos de cooperación, y del Parlamento Europeo. En particular, el artículo 25 dispone que la Agencia puede transferir datos personales a una autoridad de un país tercero o a una organización internacional «*en la medida en que dicha transmisión sea necesaria para el desempeño de las tareas de Europol*», sobre la base: «*a) de una decisión de la Comisión que establezca que el país o la organización internacional de que se trate garantizan un nivel adecuado de protección de datos (decisión de adecuación), o, a falta de*

[810] Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (*PNR*) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. Sobre dicha Directiva, *vid*. Capítulo IV.

[811] «*La limitación de la finalidad es un principio fundamental del tratamiento de datos personales; en particular, contribuye a la transparencia, la seguridad jurídica y la previsibilidad*», y es de particular «*importancia en el ámbito de la cooperación policial*», en el que las partes interesadas normalmente no son conscientes de la recopilación y del procesamineto de sus datos personales, y en el que el uso de datos personales puede tener un impacto significativo en la vida y la libertad de las personas. Considerando 26 del Reglamento Europol.

[812] Artículo 24 (Transferencia de datos personales a los organismos de la Unión) del Reglamento Europol.

una decisión de adecuación; b) de un acuerdo internacional celebrado por la Unión con arreglo al artículo 218 del TFUE, o c) de un acuerdo de cooperación que permita el intercambio de datos personales celebrado entre Europol y el país tercero de que se trate antes de la entrada en vigor del presente Reglamento»[813]. En cambio, cuando la transferencia de datos personales no se puede basar en los casos anteriores (es decir, decisión de adecuación, acuerdo internacional celebrado por la Unión o acuerdo de cooperación en vigor) el Consejo de Administración, de acuerdo con el SEPD, podrá "autorizar" una serie de transferencias si es «*a) necesaria para proteger los intereses vitales del interesado o de otra persona, o b) necesaria para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales, o c) esencial para prevenir una amenaza inminente y grave para la seguridad pública de un Estado miembro o de un país tercero, o d) necesaria en casos concretos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, o e) necesaria en casos concretos para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial relativo a la prevención, investigación, detección o enjuiciamiento de una infracción penal o la ejecución de una sanción penal específica*», teniendo en cuenta la existencia de garantías adecuadas con respecto a la protección de la intimidad y los derechos y libertades fundamentales de las personas físicas, por un período no superior a un año[814].

125. Dada la "amenaza excepcional y específica para la seguridad" interna planteada de la Unión Europea contra el terrorismo y otros delitos graves, especialmente los realizados a través de Internet, se prevé que el 1 de mayo de 2019, la Comisión evalúe la práctica de «*intercambios directos de datos personales con entidades privadas*»[815]. En el ámbito de intercambios de datos personales con entidades privadas el artículo 26, apartado 5, letra c), permite a Europol, excepcionalmente, transferir datos personales a disposición del público a entidades privadas, si se considera que la transferencia es «*estrictamente*» necesaria para el cumplimiento de esta tarea y si se refiere a un caso «*particular y específico*». Además, los derechos y las libertades fundamentales del interesado no deben prevalecer sobre el interés

[813] Artículo 25 (Transferencia de datos personales a países terceros y organizaciones internacionales), apartado 1 y 2, del Reglamento Europol. La letra c) se refiere a un acuerdo de cooperación que permite el intercambio de datos personales entre Europol y país tercero u organización internacional antes de la entrada en vigor del Reglamento (1 de mayo de 2017). El artículo 218 del TFUE establece el procedimiento para la negociación y celebración de acuerdos entre la Unión y terceros Países u organizaciones internacionales.
[814] Considerando 36 y artículo 25, apartado 5, del Reglamento Europol. También el «*director ejecutivo podrá autorizar la transferencia de datos personales a Países terceros u organizaciones internacionales*» con las mismas condiciones (apartado 6 del mismo artículo).
[815] Considerando 38 del Reglamento Europol.

público que requiere la transferencia de que se trate[816]. También, la misma disposición prevé que Europol «*podrá recibir directamente de entidades privadas datos personales que la entidad privada de que se trate declare que se le permite transmitir legalmente de conformidad con la legislación aplicable* (…)»[817].

126. El almacenamiento de datos ha sido, sin duda, uno de los aspectos más controvertidos a la hora de redactar el nuevo Reglamento Europol. Esta es una cuestión que, si ya es particularmente difícil de responder en el contexto de datos recogidos para fines comerciales, aún más lo es en el ámbito de la seguridad. Respecto al tratamiento de datos personales, que sigue representando el núcleo del funcionamiento de Europol, el Reglamento introduce algunas innovaciones significativas. El Reglamento tiene por objeto establecer un sistema de protección de datos elevado, en consonancia con la normativa de protección de datos.

127. Con este fin, en primer lugar, el artículo 28 (Principios generales en materia de protección de datos) prescribe que el tratamiento de datos personales por parte de Europol deberá ser: «*a) objeto de un tratamiento equitativo y conforme a la ley; b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados ulteriormente de forma incompatible con esos fines* (…)*; c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; d) exactos y actualizados;* (…) *e) conservados de forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que son tratados, y f) tratados de un modo que garantice una seguridad adecuada de los datos personales*». En aras de la transparencia «*Europol publicará un documento en el que se establecerán de manera inteligible las disposiciones relativas al tratamiento de los datos personales y los medios disponibles para el ejercicio de los derechos de los interesados*».

128. Los datos personales tratados por Europol sólo pueden conservarse durante el tiempo que sea necesario y proporcional a los fines para que se traten los datos[818]. El tratamiento de

[816] *Cfr*. *supra* artículo 4, apartado 1, letra m) del Reglamento Europol.
[817] Artículo 26 (Intercambios de datos personales con entidades privadas), apartado 5, del Reglamento Europol.
[818] Siempre que sea posible, los datos personales deben ser distinguidos de acuerdo con el grado de fiabilidad de la fuente de la información, utilizando códigos específicos de evaluación de fuentes definidos en el artículo 29 (Valoración de la fiabilidad de la fuente y la exactitud de la información) del Reglamento Europol. Esta disposición requiere una valoración de la fiabilidad de la fuente y una exactitud de la información, que se obtiene mediante unos códigos de evaluación de fuentes que distribuyen la información en una escala del 1 al 4 según su exactitud, y en una escala de A-B-C-X en cuanto a su fiabilidad. *Vid*. Cristina BLASI CASAGRAN

datos personales sensibles (raza, origen étnico, opiniones políticas, convicciones religiosas o filosóficas o afiliación sindical y el tratamiento de datos genéticos o datos de salud o a la vida sexual), a través de procesos automatizados o de otro tipo, está «*prohibido a menos que sea estrictamente necesario y proporcionado*» para prevenir o combatir formas de delincuencia que entren dentro de los objetivos de Europol y si esos datos complementan a otros datos personales procesados por la Agencia[819]. Sólo Europol tiene acceso directo exclusivo a los datos pertinentes.

129. Además, igual que la normativa anterior, establece que la información se debe revisar cada tres años como máximo para verificar que sigue siendo necesaria, y si no es así, debe ser cancelada de manera automática. La necesidad de "prolongar el periodo de conservación de los datos" debería revisarse dentro de los tres años siguientes al procesamiento inicial de los datos[820].

130. Para garantizar la seguridad del tratamiento de datos personales, Europol y los Estados miembros pondrán en marcha «*medidas técnicas y organizativas*» adecuadas «*para proteger los datos personales contra su destrucción accidental o ilícita, extravío accidental o divulgación, alteración y acceso no autorizados o cualquier otra forma de tratamiento no autorizado*»[821].

131. Por otra parte, se reconoce el derecho a cualquier interesado a ser informado, a intervalos razonables, de si Europol está procesando datos personales relacionados con él[822]. Sin embargo, Europol puede negar o limitar el acceso a los datos personales, "teniendo en cuenta" los derechos fundamentales y los intereses del interesado, «*si tal denegación o restricción constituye una medida necesaria*» para que Europol pueda «*desempeñar adecuadamente sus tareas*», proteger la seguridad y el orden público o prevenir delitos, garantizar que una investigación nacional se vea comprometida o «*proteger los derechos y libertades de terceros*»[823].

(2016a: 208). Artículo 31 (Plazos de conservación y cancelación de datos personales), apartados 1, del Reglamento Europol.

[819] Podrán tratarse datos personales relativos a diferentes categorías de personas implicadas, es decir, «*víctimas de delitos, testigos u otras personas*» que puedan proporcionar «*información sobre delitos*» y personas menores de dieciocho años cuando sea estrictamente necesario y proporcional para prevenir o combatir formas de delincuencia Dentro de los objetivos de Europol. *Vid*. artículo 30 (Tratamiento de categorías especiales de datos personales y de categorías diferentes de interesados), apartado 1, 2 y 3, del Reglamento Europol.

[820] Artículo 31, apartados 1, del Reglamento Europol.

[821] Artículo 32 (Seguridad del tratamiento), apartado 1, del Reglamento Europol.

[822] Artículo 36 (Derecho de acceso del interesado), apartado 1, del Reglamento Europol.

[823] Artículo 36, apartado 6, y considerando 41 del Reglamento Europol.

132. La parte interesada que tiene a los datos personales que le concierne y que Europol trata, tiene derecho a solicitar a la misma Agencia, a través de la autoridad designada a tal efecto en el Estado miembro de su elección, que "rectifique o cancele dichos datos" en poder de Europol en caso de que sean incorrectos o que hayan dejado de ser necesarios[824]. Cabe señalar que, para rectificar, cancelar o restringir los datos de las bases de datos de Europol se requiere la autorización previa del Estado miembro que facilitó tales datos originariamente[825]. Así pues, Europol no podrá eliminar estos datos si dicho Estado miembro considera que aún pueden ser relevantes a nivel nacional[826]. El artículo 37 no parece solucionar el problema más importante en cuanto a los periodos de conservación y almacenamiento de información, que es la clara dependencia a las decisiones tomadas a nivel nacional. Entonces, ¿hasta qué punto Europol tiene autoridad para decidir sobre la conservación de los datos? Una solución a esta complejidad podría ser crear un procedimiento estándar para crear criterios generales para todos los Estados miembros a la hora de decidir si conservar o no determinados datos[827].

133. En cuanto a la responsabilidad en materia de protección de datos se define en el artículo 38, que dispone que corresponde a los Estados miembros garantizar la exactitud y actualización de los datos transferidos a Europol y la legalidad de tales transferencias, mientras que Europol garantizará la exactitud y la actualización de los datos «*en el caso de los datos personales facilitados por él a los Estados miembros, países terceros u organizaciones internacionales*» (apartado 5). El Reglamento Europol establece que "cada Estado miembro designará una autoridad nacional de control". La autoridad nacional de supervisión se encargará de vigilar, de forma independiente y de conformidad con el Derecho nacional, «*la transferencia, extracción y comunicación*» de datos personales a Europol por el Estado miembro en cuestión sean lícitos y de examinar si dicha transferencia, extracción o comunicación no afectan a los derechos de los interesados[828].

[824] Artículo 37, (Derecho de rectificación, cancelación y restricción), apartados 1 y 2, del Reglamento Europol.
[825] Artículo 37, apartado 3: «*Europol restringirá, en lugar de cancelar, los datos personales contemplados en el apartado 2, en caso de que hubiera motivos razonables para suponer que la cancelación podría perjudicar intereses legítimos del interesado. Los datos restringidos solo se tratarán para los fines que impidieron su cancelación*».
[826] Artículo 37, apartado 5. De cualquier denegación de rectificación, cancelación o bloqueo por parte de Europol, las partes interesadas pueden iniciar una queja ante el SEPD y de interponer un recurso judicial (apartado 9).
[827] Cristina BLASI CASAGRAN (2016a: 209).
[828] Artículo 42 (Vigilancia por parte de la autoridad nacional de control), apartado 1, del Reglamento Europol.

134. Por cuánto atañe a la "cooperación entre el SEPD y las autoridades nacionales de supervisión", el nuevo sistema prevé, en primer lugar, la supresión de la Autoridad de Control Común (ACC)[829] cuyo papel se llevará a cabo por el Supervisor Europeo de Protección de Datos, «*con el fin de facilitar la cooperación*» entre Supervisor y las autoridades nacionales de control[830], y garantizar al mismo tiempo la eficacia y la independencia del SEPD. Él mismo vigilará y asegurará la «*aplicación de las disposiciones del Reglamento*» Europol «*relativas a la protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos personales por Europol*», y de asesorar a Europol y a los interesados sobre cualquier cuestión relativa al tratamiento de los datos personales[831]. Además, el artículo 43, apartado 3, letra f) establece que el SEPD podrá «*prohibir temporal o definitivamente las operaciones de tratamiento por parte de Europol que violen las disposiciones que rigen el tratamiento de datos personales*»[832].

135. A los nuevos poderes reconocidos a Europol, también se añaden fuertes garantías en materia de protección de datos e instrumentos de control democrático. La novedad más significativa en relación con el control democrático de la Agencia Europol viene dada por el Grupo de Control Parlamentario Conjunto (GCPC)[833], "creado conjuntamente por los parlamentos nacionales y la comisión competente del Parlamento Europeo"[834]. El GCPC efectúa «*una supervisión política de las actividades de Europol en el cumplimiento de su*

[829] Europol tenía antes de la adopción del Reglamento un órgano de control externo llamado Autoridad de Control Común (ACC), que se encontraba ubicado en Bruselas y se componía de autoridades de protección de datos de los Estados miembros.

[830] Artículo 44 (Cooperación entre el SEPD y las autoridades nacionales de control), apartado 1, del Reglamento Europol: «*El SEPD actuará en estrecha cooperación con las autoridades nacionales de control en cuestiones que requieran una intervención nacional, en particular si el SEPD o una autoridad nacional de control detectan discrepancias importantes entre las prácticas de los Estados miembros o transferencias potencialmente ilícitas en la utilización de los canales de Europol para el intercambio de información, o en el contexto de cuestiones planteadas por una o varias autoridades nacionales de control sobre la aplicación y la interpretación del presente Reglamento*».

[831] Artículo 43 (Vigilancia por parte del SEPD), apartado 1, del Reglamento Europol.

[832] Aunque el SEPD ya ha confirmado que esta prohibición será de carácter excepcional, esta cláusula ha sido criticada por Europol y por muchos Estados miembros, ya que podría obstruir investigaciones policiales en curso. Cristina BLASI CASAGRAN (2016a: 217). Además, se prevé la posibilidad de impugnar las decisiones del Supervisor ante el Tribunal de Justicia de la UE. Artículo 48 (Derecho de recurso judicial contra el SEPD), Reglamento Europol. Otra innovación es el derecho de cualquier persona que sufra un daño causado por el tratamiento ilícito de datos para obtener una indemnización tanto del Estado miembro, de conformidad con la legislación nacional, como por parte de Europol, de conformidad con el artículo 340 del TFUE. Artículo 50 (Responsabilidad por el tratamiento incorrecto de datos personales y derecho a una indemnización) del Reglamento Europol.

[833] Artículo 51 (Control parlamentario conjunto) del Reglamento Europol.

[834] De conformidad con el artículo 88 del TFUE, el control de las actividades de Europol será responsabilidad del Parlamento Europeo junto con los parlamentos nacionales. Desde el Tratado de Lisboa, el Parlamento Europeo es colegislador en las políticas del ELSJ y, por lo tanto, juega un rol muy importante en asegurarse de que las agencias del ELSJ cumplen con sus mandatos de manera efectiva.

misión» y verifica la aplicación de las disposiciones del Reglamento, en particular en relación con su impacto en los derechos y las libertades fundamentales de las personas físicas, incluso con la ayuda del SEPD[835]. El artículo 51 especifica que los procedimientos de control de las actividades de Europol por el GCPC se definirán conjuntamente por los Parlamentos nacionales y el Parlamento Europeo, de conformidad con el artículo 9 del Protocolo n. 1 sobre el papel de los parlamentos nacionales en la Unión Europea, anexo al TUE y al TFUE «*con el fin de reforzar la responsabilidad y la legitimidad democráticas de Europol ante los ciudadanos de la Unión*»[836]. El nuevo Reglamento Europol contiene normas más detalladas con respecto el acceso del Parlamento Europeo a información procesada por la Agencia o por su mediación[837].

136. De todas las novedades anteriormente descritas se puede concluir que Europol adquiere con el nuevo Reglamento ciertos poderes regulatorios. Estas nuevas funciones seguramente conllevarán una mayor eficacia y coherencia en la actividad de esta Agencia,

[835] Europol transmitirá, según el artículo 51, apartado 3, del Reglamento Europol, «*a efectos informativos, al GCPC, teniendo en cuenta las obligaciones de discreción y confidencialidad*», los siguientes documentos: «*a) valoraciones de las amenazas, análisis estratégicos e informes generales de situación relacionados con los objetivos de Europol, así como los resultados de los estudios y evaluaciones encargados por Europol; b) los acuerdos administrativos adoptados* (…)*; c) el documento que contenga la programación plurianual y el programa de trabajo anual de Europol* (…)*; d) el informe anual de actividades consolidado sobre las actividades de Europol* (…)*; e) el informe de evaluación elaborado por la Comisión* (…)». El Informe anual de actividad consolidado (CAAR) presenta los progresos realizados para alcanzar los objetivos derivados de la Estrategia de Europol y el Programa de trabajo anual. En este informe también se incluyen una descripción general de la implementación del presupuesto y la gestión de los recursos humanos, las actividades de auditoría y gestión de riesgos y la eficiencia y eficacia del sistema de control interno. Se prepara siguiendo el modelo de la Comisión de la UE y se presenta en nombre del Director Ejecutivo de Europol al Consejo de Administración para su aprobación, de conformidad con el artículo 16, apartado 5, letra g), del Reglamento Europol. De conformidad con el artículo 11, apartado 1, letra c), del Reglamento Europol, el informe tiene que ser aprobado por el Consejo de Administración que lo presenta al Parlamento Europeo, al Consejo, a la Comisión, al Tribunal de Cuentas y a los parlamentos nacionales. «Consolidated Annual Activity Report (CAAR) 2017», en *EUROPOL*. Disponible en Internet: https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2017 [consulta: 09 de agosto de 2018].

[836] Según el artículo 9 del Protocolo n. 1, «*El Parlamento Europeo y los Parlamentos nacionales definirán conjuntamente la organización y la promoción de una cooperación interparlamentaria eficaz y regular en el seno de la Unión*». En Protocolos de la Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea (2012).

[837] Artículo 52 (Acceso del Parlamento Europeo a información tratada por Europol o por su mediación) del Reglamento Europol: «*A fin de permitirle el ejercicio del control parlamentario de las actividades de Europol de conformidad con el artículo 51, el acceso del Parlamento Europeo, previa solicitud del mismo, a información sensible no clasificada tratada por mediación de Europol o por el propio Europol deberá cumplir las normas a las que se refiere el artículo 67, apartado 1*». Entonces, «*Europol establecerá normas sobre las obligaciones de discreción y confidencialidad y sobre la protección de la información sensible no clasificada*»: «*1. Europol establecerá normas sobre las obligaciones de discreción y confidencialidad y sobre la protección de la información sensible no clasificada. 2. Europol establecerá normas sobre la protección de la información clasificada de la UE que deberán ser compatibles con la Decisión 2013/488/UE, a fin de garantizar un nivel equivalente de protección de dicha información*». Artículo 67 (Normas en materia de protección de la información sensible no clasificada y clasificada) del Reglamento Europol.

la cual ahora puede hacer un mejor uso de los procesos de información disponibles, como es el caso de bases de datos e instrumentos de comunicación[838].

137. En cuanto al tratamiento de datos personales, por tanto, el Reglamento Europol parece garantizar una mayor responsabilidad de las instituciones de la UE sobre las actividades de Europol, a lo que se suma un fortalecimiento del control externo sobre la actividad de la Agencia[839].

138. Otro cambio significativo consiste en que los funcionarios de Europol podrán recibir datos de fuentes privadas, lo cual redundará en una mayor colaboración con grandes empresas, como *Microsoft*, *Apple* o *Facebook*, que sin duda ayudará a las investigaciones y a la lucha contra el terrorismo, también a través de operaciones que se iniciarán a partir de investigaciones web.

139. Finalmente, la UE se enfrenta a enormes desafíos de seguridad y éstos nos exigen, más que nunca, atenernos a nuestros valores, nuestros derechos y libertades fundamentales. Nace una necesidad urgente de que los Estados miembros de la UE mejoren el análisis y el intercambio eficiente de información y defiendan los valores y libertades establecidos en la CDFUE. El nuevo Reglamento Europol moderniza el marco para compartir información, el análisis de inteligencia y evaluaciones de amenazas[840]. También es oportuno, coincidiendo con la reciente adopción del RGPD y la Directiva de protección de datos para asuntos policiales y judiciales. El nuevo Reglamento aumenta la responsabilidad de la Agencia y confirma el fuerte régimen de protección de datos de Europol. El nuevo Reglamento parece garantizar un régimen sólido de protección de datos para Europol y proporciona a la agencia

[838] Cristina BLASI CASAGRAN (2016a: 207).

[839] Para evitar que haya brechas en la información relacionada con el crimen organizado y el terrorismo, las nuevas normas exigen a los Estados miembros proporcionar a Europol los datos necesarios. Para fomentar el intercambio de información, Europol informará anualmente al Parlamento Europeo, al Consejo, a la Comisión y a los Parlamentos nacionales de la información proporcionada por los distintos Estados miembros.

[840] La necesidad de una mayor coordinación en la lucha contra la aplicación a los fenómenos de la delincuencia organizada y el terrorismo que han llevado a los Estados miembros de la UE a enfrentarse sobre diversos temas como el intercambio de información, la creación de una agencia de seguridad europea con plenos poderes de investigación especializada en la lucha contra el terrorismo, las revisiones de los controles fronterizos, los controles previstos en los aeropuertos. En enero de 2016 se ha fortalecido el mandato de Europol, con la creación del Centro Europeo de Lucha contra el Terrorismo (*European Counter-Terrorism Centre - ECTC*). Se trata de un centro de información centralizado que contribuye al intercambio de información entre las fuerzas policiales de los Estados miembros, en relación con la identificación de los combatientes extranjeros ("*foreign fighters*"), en contraste con las diversas formas de financiación del terrorismo, de la propaganda terrorista en línea y el tráfico internacional de armas. Consulte la página web de Europol sobre ECTC: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.

un sistema de gestión de datos flexible y moderno[841], que permitirá a Europol mejorar su apoyo a los Estados miembros en la lucha contra el terrorismo y la delincuencia organizada.

[841] El Reglamento elimina los tres sistemas de tratamiento de información para dar apoyo a los Estados miembros, que consistían en los Ficheros de Trabajo de Análisis (FTAs), el Sistema de Información de Europol (SIE) y la Función de Índice. La nueva forma de tratar la información que llega con el Reglamento (UE) 2016/794 a Europol se describe como un único canal en el que se procesan todos los datos, y no varios sistemas de datos como ocurría en la Decisión del Consejo anterior. Todos estos sistemas se han fusionado en uno, que se compone de diferentes condiciones según el tipo y categoría de datos que traten, así como de su finalidad específica (Anexo 2 de Reglamento Europol).

CAPÍTULO IV

LA TENSIÓN ENTRE PRIVACIDAD Y SEGURIDAD EN LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

1. El TJUE en la construcción del derecho fundamental a la protección de datos de carácter personal

1. El sistema de protección de datos en el ámbito de la Unión Europea se asienta en el contenido de los Tratados y de la CDFUE, así como en la normativa que en este ámbito los desarrollan. No obstante, en un sistema jurídico con las características de la Unión resulta imprescindible hacer referencia a la jurisprudencia del TJUE no sólo porque es la institución que garantiza el respeto del derecho en la interpretación y aplicación de los Tratados[842], sino porque en los años ha desarrollado, y continúa desempeñando, un papel creativo del derecho, en particular en el tema específico de los derechos fundamentales que no se recogen de manera expresa en los Tratados[843].

2. El TJUE ejerce una función de equilibrio, solucionando los conflictos en los casos específicos que se someten a su conocimiento, interpretando el derecho de la UE, del que garantiza una interpretación uniforme en todos los países de la UE. Sobre la base de las decisiones del legislador europeo, su objetivo es encontrar el equilibrio adecuado y la correcta ponderación de las diversas exigencias en cada caso, y, por lo que interesa a la presente investigación, el equilibrio entre seguridad y protección de datos a partir de los textos legales, en cuya búsqueda llega a criticar la falta de consideración de las cuestiones

[842] Artículo 19 del TUE: «*1. El Tribunal de Justicia de la Unión Europea comprenderá el Tribunal de Justicia, el Tribunal General y los tribunales especializados. Garantizará el respeto del Derecho en la interpretación y aplicación de los Tratados. Los Estados miembros establecerán las vías de recurso necesarias para garantizar la tutela judicial efectiva en los ámbitos cubiertos por el Derecho de la Unión*».

[843] El Acta Única Europea de 1986 sólo indica en el preámbulo la promoción de la democracia basada en los derechos fundamentales; sólo con el Tratado de Maastricht de 1992 se establece una norma, el artículo F del TUE, que se ha convertido en el artículo 6 con el Tratado de Ámsterdam y modificado por el Tratado de Lisboa. Con esta norma, la protección de los derechos fundamentales está consagrada en la legislación de la UE. Hasta entonces, el TJUE había definido las obligaciones de los Estados e instituciones en la aplicación del Derecho comunitario y, por otro, los derechos de los particulares en lo que respecta a la protección de los derechos fundamentales. Por lo tanto, el TJUE, creado en 1952, con el Tratado de Lisboa ha ampliado su alcance jurisdiccional. *Vid*. Bruno NASCIMBENE (2016), «La tutela dei diritti fondamentali nella giurisprudenza della Corte di giustizia», en *Convegno in occasione dei primi 25 anni della Rivista italiana di diritto pubblico comunitario, Diritto europeo e diritti amministrativo nazionale 25 anni dopo*, in data 11.11.2016. pág. 1. Disponible en Internet: http://rivista.eurojus.it/la-tutela-dei-diritti-fondamentali-nella-giurisprudenza-della-corte-di-giustizia/ [consulta: 18 de septiembre de 2017].

relativas a los derechos fundamentales en el proceso de armonización de la UE que se centra exclusivamente en los aspectos técnicos de la retención de datos.

3. En su actividad jurisprudencial, el TJUE se ha enfrentado muchas veces con el tema de la protección de los datos personales[844]. De hecho, cada vez que los Estados miembros no quieren progresar en el proceso de enriquecimiento del *acquis* comunitario a través de la adopción de nueva normativa, el TJUE asume una función activa y la materia evoluciona gracias a la acción judicial. Las sentencias del Tribunal en este ámbito son las que permiten confirmar que, para el ordenamiento jurídico de la UE, la protección de datos es, hoy en día, un derecho fundamental real y efecto de los ciudadanos[845].

4. Por lo tanto, la definición actual del derecho a la privacidad y a la protección de datos en el ámbito de la UE es deudora, en gran medida, de la jurisprudencia del TJUE, por lo que se trata del caso típico de un derecho fundamental que nació de una forma «*pretoriana*»[846],

[844] Para una visión completa de la opinión del TJUE en relación con la protección de datos, véase Artemi RALLO LOMBARTE (2017), «El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet», en *UNED. Teoría y Realidad Constitucional*, núm. 39, pág. 584. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19150 [consulta: 19 de septiembre de 2017]; Gemma MINERO ALEJANDRE (2017), «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», en *Anuario Jurídico y Económico Escurialense*, págs. 13-58. ISSN: 1133-3677; José Luis PIÑAR MAÑAS y Miguel RECIO GAYO (2018), *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Madrid, Wolters Kluwer – La Ley, págs. 300; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[845] La jurisprudencia del TJUE sobre la protección de los derechos fundamentales se remonta a finales de los años sesenta y principios de los setenta, a falta de una disposición expresa de los Tratados. Bruno NASCIMBENE (2016: 4). El primer caso en el que el TJUE se pronuncia sobre los derechos fundamentales es en el caso *Stauder*. La Corte ha reconocido en la intimidad un derecho fundamental de la persona que hace parte a los principios generales del derecho comunitario de que ella es llamada a garantizar la observancia. En el presente caso, aunque el TJUE no hace referencia expresa a un derecho a la protección de datos personales, si entendemos, como ha hecho el TEDH, que el nombre es un dato personal que forma parte de la vida privada estamos ante un caso de protección de datos personales donde se produce la cesión a los vendedores. *Vid*. TJUE, *Erich Stauder contra Stadt Ulm - Sozialamt*, asunto 29/69, sentencia de 12 de noviembre de 1969. Más adelante, en los casos *Internationale Handelsgesellschaft* y, de forma más clara, desde el caso *Nold*, se afirma ya la protección de los derechos fundamentales como parte integrante del derecho comunitario con expresa referencia a las tradiciones constitucionales comunes y a los tratados internacionales sobre derechos fundamentales. En particular, en el caso *National Panasonic (UK) Limited*, el Tribunal ha extendido también a las personas jurídicas la tutela tradicionalmente concedida por los derechos fundamentales a los datos personales, el domicilio y la correspondencia de los individuos. *Cfr*. TJUE, *Internationale Handelsgesellschaft mbH contra Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, asunto 11/70, sentencia de 17 de diciembre de 1970. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61970CJ0011&from=ES [consulta: 15 de febrero de 2016]; TJUE, *J. Nold, Kohlen-und Baustoffgroßhandlung contra Commission des Communautés européennes*, asunto 4-73, sentencia de 14 de mayo de 1974. Disponible en Internet: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?isOldUri=true&uri=CELEX:61973CJ0004 [consulta: 13 de febrero de 2016]; TJUE, *National Panasonic (UK) Limited contra Comisión de las Comunidades Europeas*, asunto 136/79, sentencia de 26 de junio de 1980.

[846] *Vid*. Rafael GARCÍA-VALDECASAS Y FERNÁNDEZ, José María CARPI BADÍA (2004), «El Tribunal de Justicia de la Unión Europea. Algunas consideraciones respecto a su papel en el marco de la construcción europea», en *Revista Jurídica de Castilla y León*, núm. 3, págs. 32 y ss. Disponible en Internet: http://portaljuridico.lexnova.es/revista-castilla-leon/documento/760/6737/el-tribunal-de-justicia-de-la-union-

a través del *ius praetorium* creado por el mismo juez, antes de ser positivizados, desempeñando un papel clave en la construcción del sistema comunitario.

5. La protección de los derechos fundamentales[847] es una de las cuestiones que ha permitido al TJUE afirmar el principio de primacía, eficacia directa[848], unidad del ordenamiento jurídico europeo e interpretación uniforme garantizada por el Tribunal, definiendo las relaciones entre el Derecho nacional de los Estados miembros y el Derecho de la Unión y la relación entre las distintas fuentes: Tratados y CEDH. De hecho, permitió el inicio de una comparación o "diálogo entre los Tribunales"[849], los Tribunales Constitucionales y el TEDH; un diálogo, en el ámbito de los derechos fundamentales, que se convierte en una "triangulación"[850]. Por lo tanto, el TJUE ha llegado a reconocer la protección de datos personal, como parte de un sistema de protección multinivel[851], que

europea-algunas-consideraciones-respecto-a-su-papel-en-el-marco [consulta: 06 de enero de 2016]; Teresa FREIXES SANJUÁN (2005); Mónica ARENAS RAMIRO (2008: 117).

[847] Hay que aclarar que, el TJUE, en su papel de proteger los derechos fundamentales, por un tiempo fue llamado por casos de matriz esencialmente económica, emancipado gradualmente de esta su dimensión original debido a las referencias cada vez más frecuentes al TEDH y las tradiciones constitucionales comunes a los Estados miembros; hasta la incorporación de la Carta de Niza y Estrasburgo en el Tratado de Lisboa. Por lo tanto, se parte de una Comunidad Económica para llegar a la Unión, donde se ha ampliado la integración entre Estados con la centralidad de los derechos del individuo gracias a la jurisprudencia que formuló su posición dentro del ordenamiento europeo, y, sobre todo, a las modificaciones de los Tratados que, siguiendo las indicaciones del TJUE, protegen de forma directa (y sin excepción) los derechos fundamentales de la persona, estableciendo derechos específicos del ciudadano de la Unión, reconocen el efecto vinculante de la CDFUE (artículo 6, apartado 1, del TUE). Véase por todos, Giancarlo ROLLA (2010), «La Carta de Derechos Fundamentales de la Unión Europea y el Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales: su contribución a la formación de una jurisdicción constitucional de los derechos y las libertades», en *Revista Europea de Derechos Fundamentales*, núm. 15, págs. 15-39. Disponible en Internet: http://journals.sfu.ca/redf/index.php/redf/article/viewFile/236/229 [consulta: 06 de septiembre de 2017].

[848] Es la Corte la que afirma los principios de primacía (sentencia *Costa contra Enel*, de 1964) y el efecto directo (sentencia *Van Gend en Loos*, de 1963), que define las características de la Unión como un «*ordenamiento jurídico de una nueva índole, con una naturaleza específica*» (dictamen 2/13 de 18.12.2014). Estas características están destinadas a mantenerse en el tiempo, a pesar de las pretensiones de soberanía expresadas explícita o implícitamente por algunos Estados miembros. Vid. TJUE, *Costa contra Enel*, asunto 6/64, sentencia de 15 de julio de 1964. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61964CJ0006&from=IT [consulta: 07 de septiembre de 2017]; TJUE, *NV (Sociedad Anónima) Algemene Transport- en Expeditie Onderneming van Gend & Loos contra Nederlandse administratie der belastingen (Administración Tributaria neerlandesa)*, asunto 26/62, sentencia de 5 de febrero de 1963; y Dictamen del Tribunal de Justicia (Pleno) de 18 de diciembre de 2014. Dictamen emitido en virtud del artículo 218 TFUE, apartado 11. Dictamen 2/13.

[849] Con respecto al diálogo judicial en el ámbito europeo, vid. Miryam RODRÍGUEZ-IZQUIERDO SERRANO (2015), «El Tribunal de Justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a libertades informativas», en *Revista de Derecho Constitucional Europeo*, año 12, núm. 24, julio-diciembre. ISSN: 1697-7890; Juan Fernando LÓPEZ AGUILAR (2017: 559).

[850] Expresión de Bruno NASCIMBENE (2016: 3).

[851] *Vid*. Oreste POLLICINO (2010), «The New Relationship between National and the European Courts after the Enlargement of Europe: Towards a Unitary Theory of Jurisprudential Supranational Law?», en *Yearbook of European Law*, vol. 29, issue 1. Disponible en Internet: https://doi.org/10.1093/yel/29.1.65 [consulta: 08 de diciembre de 2015]; Marta CARTABIA (2014), «La tutela multilivello dei diritti fondamentali. Evoluzioni della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona», en *Incontro trilaterale tra le Corti costituzionali italiana, portoghese e spagnola*, Santiago de Compostela, 16-18 ottobre 2014, págs. 21. Disponible en Internet: http://docplayer.it/1121975-La-tutela-multilivello-dei-diritti-fondamentali.html [consulta: 29 de enero de 2016].

caracteriza la situación actual de todos los derechos fundamentales en Europa y que se distingue por la multiplicidad de fuentes de reconocimiento de los derechos y la extensión de sus ámbitos de protección[852], quedando garantizados en el derecho vivo que surge de los diversos Tribunales. Se delinea así el perímetro dinámico de un diálogo entre Tribunales que alimenta la cultura de un Derecho Común europeo[853]. Por esta razón, como veremos, el TJUE en materia de protección de datos de carácter personal sigue en gran medida el camino ya trazado por las sentencias del TEDH sobre la base del CEDH y otros instrumentos internacionales en el marco del Consejo de Europa.

6. Si bien el primer período de actividad del TJUE en materia de protección de datos y la privacidad[854] se caracteriza por su amplia referencia a las disposiciones del CEDH[855] y las decisiones del TEDH, en tiempos más recientes el TJUE parece más orientado hacia el uso de reconocimiento y valoración de su propio criterio, ejerciendo un intenso control sobre la legitimidad de cualquier restricción de los derechos fundamentales. Esta tendencia parece

[852] A falta de un catálogo expreso, los jueces europeos han establecido los derechos fundamentales que merecen protección por el Derecho europeo, utilizando la categoría de "principios generales del Derecho comunitario". En esta acción han recurrido a las "tradiciones constitucionales comunes de los Estados miembros", además a los Tratados internacionales y en particular la CEDH. *Amplius*, Marta CARTABIA (2007: 13 y ss).

[853] *Vid*. Ricardo ALONSO GARCIA (1989), *Derecho Comunitario, Derechos Nacionales y Derecho Común europeo*, Madrid, Editorial Civitas, págs. 322; Alejandro SÁIZ ARNAIZ (2005), «El Tribunal de Justicia, los Tribunales Constitucionales y la tutela de los derechos fundamentales en la Unión Europea: entre el (potencial) conflicto y la (deseable) armonización: de los principios no escritos al catálogo constitucional, de la autoridad judicial a la normativa», en Itziar GÓMEZ FERNÁNDEZ (coord.), Marta CARTABIA, Bruno DE WITTE, Pablo PÉREZ TREMPS (dir.), *Constitución europea y constituciones nacionales*, Valencia, Tirant lo Blanch, págs. 531-588; Ana CARMONA CONTRERAS (2016), «El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales», en *Revista Española de Derecho Constitucional*, núm. 107, págs. 13-40. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5634735 [consulta: 19 de septiembre de 2017].

[854] Como demuestran los estudios más recientes de la doctrina, se señalan al menos tres ámbitos específicos de incidencia decisiva de la jurisprudencia del TJUE sobre la de los tribunales garantes de los ordenamientos de los Estados miembros: el acceso a la Justicia y a la tutela judicial; la igualdad de trato y no discriminación; y, en lo que nos interesa, privacidad, vida privada y protección de datos. *Vid*. Juan Fernando LÓPEZ AGUILAR (2017).

[855] Durante la primera mitad de los noventa, el TJUE ha afirmado la incidencia del derecho a la tutela de los datos en el ámbito de la vida privada y familiar, comenzando a reconocer el artículo 8 del CEDH en relación con la protección de los datos personales y recordar la jurisprudencia del TEDH, utilizando como criterios de juicio los mismos requisitos del CEDH que pueden justificar la interferencia en la vida privada. Esta injerencia o limitación, entendida en los términos de la jurisprudencia del TEDH, sólo puede ser compatible con lo dispuesto en los artículos 8, apartado 2 y 9, apartado, cuando se establece por ley que persigue uno o más de los objetivos legítimos allí recogidos y cumple el requisito de necesidad en una sociedad democrática. Con la primera norma en materia de protección de datos personales, la Directiva 95/46/CE, resultará determinante para el reconocimiento y desarrollo del derecho a la protección de datos personales, que el Tribunal utilizará como piezas de su razonamiento. Esta norma se convierte en el segundo elemento, después de la jurisprudencia del TEDH, que alimenta la jurisprudencia del TJUE en la materia. Las decisiones en esta materia siguen en gran parte el surco ya trazado por las pronunciaciones del TEDH sobre la base del CEDH y otros instrumentos internacionales en el marco del Consejo de Europa. TJUE (Gran Sala), *Comisión Europea contra The Bavarian Lager Co. Ltd, Supervisor Europeo de Protección de Datos (SEPD)*, asunto C-28/08 P, sentencia de 29 de junio de 2010.

confirmarse en su función de control de las normativas europea y nacional[856] -dentro de los límites, pero en realidad no trazado con precisión por el artículo 51, apartado 1, de la Carta[857]- a la luz de los derechos fundamentales y los principios de necesidad, proporcionalidad y legitimidad de la finalidad ("*purpose limitation*"), junto a la delimitación temporal de la retención y conservación de datos ("*retention period*")[858], al operar una tendencia ya especificada en la jurisprudencia del TEDH, por lo tanto mostrando, una vez más, la intención de relanzar su papel de garante del respeto de los derechos fundamentales dentro de la de la Unión, en una perspectiva, sin embargo, de diálogo continuo y fructífero con otros Tribunales con la misma función, es decir, el TEDH y los Tribunales Constitucionales nacionales[859].

7. En efecto, el TJUE no sólo se ha limitado a inspirarse en la jurisprudencia del TEDH sobre la protección de datos personales, sino que procedió también a incorporarla directamente en sus decisiones. La jurisprudencia en este ámbito se caracteriza por un enfoque integral en la protección de la privacidad que se realiza por referencia, con frecuencia acumulada, a los artículos 7 y 8 de la CDFUE[860], sin llevar a cabo claramente la

[856] *Vid*. los casos *Fransson* y *Melloni*: TJUE (Gran Sala), *Åklagaren y Hans Åkerberg Fransson*, asunto C-617/10, sentencia de 26 de febrero de 2013; TJUE (Gran Sala), *Stefano Melloni y Ministerio Fiscal*, asunto C-399/11, sentencia de 26 de febrero de 2013.

[857] Artículo 51 (Ámbito de aplicación), apartado 1, de la CDFUE: «*Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que se atribuyen a la Unión*». Sobre la interpretación del artículo 51 de la Carta, vid. Eleanor SPAVENTA (2016), «The interpretation of Article 51 of the EU Charter of Fundamental Rights: the dilemma of stricter or broader application of the Charter to national measures», en *Study commissioned by the Policy Department for Citizen's Rights and Constitutional Affairs at the request of the PETI Committee*, PE 556.930, págs. 38.

[858] Juan Fernando LÓPEZ AGUILAR (2017: 561).

[859] Sobre las particularidades de este asunto, puede verse Javier DÍEZ-HOCHLEITNER (2013), «El derecho a la última palabra: ¿Tribunales constitucionales o Tribunal de Justicia de la Unión?», en *Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense Facultad de Derecho*, Papeles de Derecho Europeo e Integración Regional, núm. 17, págs. 38. ISSN: 2172-8542. Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2013-11-07-el%20derecho%20a%20la%20%C3%BAltima%20palabra.pdf [consulta: 30 de enero de 2016]; Juan Ignacio UGARTEMENDIA ECEIZABARRENA (2013), «La tutela judicial de los derechos fundamentales en el ámbito de aplicación nacional del derecho de la Unión Europea: recientes acotaciones del Tribunal de Justicia y del Tribunal Constitucional Español», en *UNED. Teoría y Realidad Constitucional*, núm. 32, págs. 391-428. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/11796 [consulta: 19 de enero de 2016].

[860] En combinación con el derecho a la tutela judicial efectiva y a un juez imparcial, reconocida por el artículo 47 de la CDFUE: «*Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia*».

autonomía conceptual del derecho a la protección de los datos personales con el tradicional derecho al respeto de la vida privada. Además, hasta el momento en que se planteó la cuestión de las limitaciones permitidas a los derechos previstos en los artículos 7 y 8 de la CDFUE, con referencia a la aplicación del artículo 52 de la Carta[861], el TJUE no distinguía el perfil a la aplicación del principio de proporcionalidad, de aquel relativo a la infracción del «*contenido esencial*» de los derechos en juego[862].

8. Así, la conservación de datos puede ser una limitación del derecho al respeto de la vida privada y el derecho a la protección de datos personales. En paralelo con el artículo 8, apartado 2, del CEDH, la Carta reconoce que la injerencia de la autoridad pública en el ejercicio del derecho al respeto de la vida privada puede estar justificada si resulta necesaria para la "seguridad nacional", la "seguridad pública" y "prevención de delitos". En particular, en virtud del artículo 52, apartado 1, estas limitaciones «*deberán ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás*»[863].

---

[861] Como es bien sabido, la CDFUE representa un punto de inflexión en el tema de la protección de los derechos, en tanto es un catálogo finalmente adoptado después de un largo debate sobre si se debía o no adoptar un catálogo. No se superpone al CEDH, sino que más bien se coordinan. En este sentido, el artículo 52, apartado 3, de la CDFUE establece que: «*En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa*».

[862] En este sentido, resulta significativo el razonamiento del TJUE en la sentencia *Volker* de 2010. De hecho, hay que considerar que, por una parte, «*el respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal, reconocido por los artículos 7 y 8 de la Carta, se aplica a toda información sobre una persona física identificada o identificable*» y, por otra, «*que las limitaciones al derecho a la protección de los datos de carácter personal que pueden establecerse legítimamente corresponden a las toleradas en el contexto del artículo 8 del CEDH*». La referencia al artículo 8, «*se halla íntimamente ligado al derecho al respeto de la vida privada, consagrado en el artículo 7 de dicha Carta*». TJUE (Gran Sala), *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *y Land Hessen*, asuntos acumulados C-92/09 y C-93/09, sentencia de 9 de noviembre de 2010, apartados núms. 52 y 47.

[863] Cabe señalar, también, que el TJUE, antes de las recientes sentencias de los últimos años, nunca había mencionado ni la cláusula de correspondencia prevista por la Carta de Niza que figura en el artículo 52, apartado 3, ni la cláusula sobre el nivel de protección del artículo 53 de la Carta, evitando comparar cualquier excepción por la Directiva 95/46/CE para justificar una invasión en la privacidad con los supuestos previstos en el CEDH. De esta manera se preserva su libertad, en casos futuros, para llegar a un equilibrio diferente de la operada por el Tribunal de Estrasburgo, en caso de detectar una extensión del derecho protegido a nivel comunitario distinto de la prevista en el sistema CEDH. Artículo 53 (Nivel de protección) de la CDFUE: «*Ninguna de las disposiciones de la presente Carta podrá interpretarse como limitativa o lesiva de los derechos humanos y libertades fundamentales reconocidos, en su respectivo ámbito de aplicación, por el Derecho de la Unión, el Derecho internacional y los convenios internacionales de los que son parte la Unión, la Comunidad o los Estados miembros, y en particular el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como por las constituciones de los Estados miembros*».

9. A partir de este fundamento las sentencias del TJUE han fijado claramente las características de estas eventuales limitaciones: "deben ser formuladas con precisión y previsibilidad; necesarias para alcanzar un objetivo de interés general o para proteger los derechos y libertades de los demás; proporcionadas al objetivo perseguido"; conformes a la esencia de los derechos fundamentales de lo que se trata. Por tanto, la protección de los datos personales según lo dispuesto por la obligación establecida por el artículo 8, apartado 1, de la CDFUE es particularmente importante para el derecho al respeto de la vida privada en virtud del artículo 7 de la misma Carta[864].

10. Las decisiones jurisprudenciales demuestran que el derecho a la privacidad y la necesidad de su protección homogénea en toda Europa ha evolucionado y ha llegado a afirmarse de manera muy decisiva, gracias al diálogo constante entre legisladores y tribunales, que ha permitido ampliar el alcance del derecho a la privacidad incluso en el contexto de los graves desafíos para la seguridad que han supuesto los constantes ataques terroristas. En este sentido, el TJUE ha emitido algunos pronunciamientos recientes en los últimos años sobre el impacto significativo de las políticas que se han aplicado hasta ahora.

11. En este sentido, la actividad del Tribunal se ha centrado en la búsqueda continua de un equilibrio aceptable entre diferentes valores y principios que no son fácilmente conciliables entre sí: la salvaguardia de la confidencialidad con las exigencias relacionadas con la seguridad, lo que nos interesa, para contrastar las diversas formas de delincuencia y terrorismo que pueden utilizar las herramientas informáticas, y las exigencias del mercado con la ampliación en términos de las oportunidades comerciales y los posibles beneficios en términos de reducción de costos para los usuarios. Al mismo tiempo, el TJUE se convierte en uno de los instrumentos que puede servir de límite a los excesos de los gobiernos y legisladores en la lucha antiterrorista[865]. Por lo tanto, las críticas del TJUE se

[864] Entre las dos normas, como se ha indicado anteriormente, el artículo 8 está dotado de mayor alcance innovativo, como la anticipación de un verdadero derecho de los datos personales. Por un lado, consiste en una "constitucionalización" del derecho a la protección de datos personales, y por otro, un despegue definitivo de su vinculación a la dimensión económica de la consolidación del mercado interior que caracterizó el significado jurídico de la Directiva 95/46/CE. Sobre la consolidación gradual de un "núcleo constitucional" por el TEDH, el TJUE y Tribunales Constitucionales nacionales, vid. Oreste POLLICINO, Graziella ROMEO (2016), *The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe*, New York, Routledge, págs. 264.

[865] Especialmente sobre la transferencia continua y constante de datos que domina la sociedad actual no se puede subestimar el marco internacional que se esbozó después del 11 de septiembre de 2001. La relación entre la seguridad nacional y la privacidad siempre ha aparecido conflictiva, y ha llegado a resolverse a favor en gran medida de la seguridad nacional dada la constante y grave amenaza del terrorismo internacional. En este contexto, los tribunales han tenido que desarrollar un papel no simple para conciliar el derecho a la protección de datos personales con otros derechos e intereses en juego. Debe recordarse que, después del 11 de septiembre,

han concentrado en el uso incorrecto del margen de la apreciación que, en principio, disfrutan las autoridades públicas (nacionales y europeas) para incidir en los derechos fundamentales de manera legítima[866]. En efecto, entre los instrumentos que pueden servir de límite a los excesos de los gobiernos y legisladores y como garantía de la protección de los derechos fundamentales en la lucha antiterrorista[867], el TJUE es uno de ellos. Por esa razón,

---

la respuesta del gobierno de EE.UU. a los ataques terroristas fue la adopción de la Ley Patriota (*Patriot Act*), que redefinió el marco legal de los derechos de los ciudadanos, dejando prioridad a la seguridad nacional antes que a que cualquier otro derecho fundamental como, en primer lugar, el derecho a la privacidad. A través de esta intervención reguladora, de hecho, se han aumentado los poderes de intervención de los servicios de inteligencia y las posibilidades por parte de éstos, para explotar el potencial que ofrecen los datos.

[866] El TJUE, ya desde los años setenta, fue introduciendo un juicio de ponderación entre ese mantenimiento de la seguridad y el respeto de los derechos y libertades. Desde el 1974, con el fallo *Van Duyn*, el Tribunal sostuvo que, si bien la definición de los límites del concepto de orden público es una prerrogativa del Estado, cuando este concepto se utiliza para establecer excepciones a una libertad fundamental consagrada en el Tratado, puede ser interpretado de manera restrictiva; en consecuencia, el Tribunal ejerce su control. Tal posición se ha desarrollado en diferentes direcciones, todas tendentes a limitar la arbitrariedad de la aplicación de la excepción de los Estados esencialmente basados en dos principios, que también se informó toda la legislación secundaria: de proporcionalidad y no discriminación. Vid. TJUE, *Yvonne van Duyn y Home Office*, asunto 41/74, sentencia de 4 de diciembre de 1974. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61974CJ0041&from=IT [consulta: 26 de enero de 2016]. La primera decisión relevante sobre el juicio de ponderación entre mantenimiento de la seguridad y el respeto de los derechos y libertades, en ese sentido, se produjo en el caso *Rutili*, en el que el TJUE, además de introducir límites explícitos en la discreción de los Estados al adoptar medidas para salvaguardar el orden público, puso como condición para la aplicación de la restricción a la libertad de circulación en una parte del territorio el hecho de que la medida pudiera ser tomada por los Estados miembros contra ciudadanos de la UE, así como hacia sus ciudadanos. El caso trataba de la decisión del Ministerio del Interior francés de prohibir a un ciudadano de origen italiano el acceso a algunos departamentos franceses, a causa de sus actividades políticas y sindicales. En este caso, el Tribunal formuló por primera vez el principio de proporcionalidad en relación con las medidas de interdicción a la libertad de movimiento como un principio general del derecho y, al mismo tiempo, afirmó que el comportamiento de la persona objeto de la medida restrictiva debe constituir una amenaza real y suficientemente grave para el orden público. TJUE, *Rolland Rutili y Ministerio del Interior*, asunto 36/75, sentencia de 28 de octubre de 1975. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61975CJ0036&from=FR [consulta: 29 de enero de 2016]. En el caso *Rutili* el Tribunal declaró que: «*la justificación de las medidas destinadas a salvaguardar el orden público deberá ser valorada tomando en consideración todas las normas de Derecho comunitario que tengan por objeto, por una parte, limitar la apreciación discrecional de los Estados miembros en la materia, y, por otra parte, garantizar la defensa de los derechos de las personas sujetas a medidas restrictivas por razones de orden público*» (apartado 51) y que «*un Estado miembro sólo podrá imponer a los nacionales de otros Estados miembros (a los que se aplican las disposiciones del Tratado) medidas restrictivas del derecho de residencia limitadas a una parte del territorio nacional en los casos y en las condiciones en que tales medidas puedan aplicarse a los nacionales del Estado de que se trate*» (apartado 53). Magdalena M. MARTÍN MARTÍNEZ (2014), «Límites a la libre circulación de personas en la UE por razones de orden público, seguridad o salud pública en tiempos de crisis: una revaluación a la luz de la jurisprudencia del TJUE», en *Revista de Derecho Comunitario Europeo*, núm. 49, septiembre/diciembre, págs. 774-783. ISSN 1138-4026.

[867] El TJUE siempre ha invocado el legado común europeo en materia de derechos humanos y el imperio de la ley. En el caso *Ocalan*, el Tribunal recordó que: «*la Comunidad Europea es una comunidad de Derecho cuyas instituciones están sujetas al control de la conformidad de los actos que adoptan con el Tratado y con los principios generales del Derecho, de los que forman parte los derechos fundamentales. Por consiguiente, los particulares deben poder disfrutar de una tutela judicial efectiva de los derechos que les confiere el ordenamiento jurídico comunitario, ya que el derecho a dicha tutela forma parte de los principios generales del Derecho que resultan de las tradiciones constitucionales comunes a los Estados miembros. Este derecho también ha sido consagrado en los artículos 6 y 13 del CEDH*». TJUE (Sala Primera), *Osman Ocalan, Serif Vanly y Consejo de la Unión Europea*, asunto C-229/05 P, sentencia de 18 de enero de 2007, apartado 109. El Tribunal reconoció en el caso citado que, si bien la normativa nacional puede establecer medidas restrictivas dirigidas contra determinadas personas y entidades con el fin de luchar contra el terrorismo, cabe establecer limitaciones a esas facultades de los Estados miembros. *Vid*. Rosario SERRA CRISTÓBAL (2015a: 44). Una de las dificultades con la que se enfrenta el TJUE en materia de terrorismo reside en que sólo tiene competencia

como se ha afirmado, el TJUE se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global[868].

12. Por lo tanto, tanto a nivel interno como de la UE, el TJUE desempeña un papel de fiscalización que puede convertirse en una de las mejores garantías para la protección de los derechos fundamentales. Esto es consecuencia inmediata de la inacción o insuficiencia por parte del legislador europeo, que "obliga" al Tribunal a responder de una manera decisiva, cuya acción ha dado lugar a un impulso creativo con la adopción de una decidida reglamentación de la protección de un nuevo derecho para la privacidad, sobre todo a partir de mayo de 2016 con la adopción del "Paquete de protección de datos", constituido por el nuevo RGPD, así como por la Directiva que establece específicamente estos principios en las actividades judiciales y policiales (Directiva 2016/680). Lo que, en sí mismo, pone de relieve la voluntad de positivizar el derecho a la privacidad y la necesidad de su protección homogénea en toda Europa[869].

13. En todo caso, el Tribunal de Luxemburgo lleva desempeñando desde hace años un papel en favor de la promoción de los derechos en la lucha contra el terrorismo. Y ello, pese a que el TJUE es un "recién llegado" al campo de la lucha contra el terrorismo y otros asuntos de seguridad nacional, si lo comparamos con el TEDH o los tribunales nacionales que se han ocupado desde siempre de esta materia[870].

14. Resulta ejemplar en este sentido tres pronunicamientos del TJUE en los que se va a centrar el presente Capítulo y que fueron adoptados en el período 2014-2016, y que han

indirecta y limitada sobre la Política Exterior y de Seguridad Común. Sin embargo, desde 1 de diciembre de 2014, tiene plena jurisdicción sobre Cooperación Policial y Judicial (Intercambio de información, la cooperación antiterrorista, extradiciones/detención, lucha contra el crimen organizado, *etc*.). En esa fecha finalizó el período transitorio de cinco años previsto en el Tratado de Lisboa para las limitaciones al control judicial por el TJUE sobre la cooperación judicial y policial en materia penal de los Estados miembros, así como sobre la función de la Comisión como guardiana del Tratado en el ámbito de la cooperación judicial en materia penal. Por tanto, en la actualidad el TJUE dispone ya de plena jurisdicción sobre la ejecución de la cooperación judicial y policial en materia penal, y la Comisión puede iniciar un procedimiento de infracción contra cualquier Estado miembro que infrinja el Derecho de la Unión, si no lo aplica correctamente. *Vid*. COMISIÓN EUROPEA - Comunicado de prensa (2014), Una nueva era para las políticas de justicia e interior de la UE, Bruselas, 01 diciembre 2014. Disponible en Internet: http://europa.eu/rapid/press-release_IP-14-2266_es.htm [consulta: 01 de febrero de 2016].

[868] Artemi RALLO LOMBARTE (2017: 584).

[869] Hasta la aprobación de las nuevas normas europeas, nos hemos enfrentado no sólo con unas normas europeas (ej. Directiva 95/46/CE y Decisión Marco 2008/977/JAI) al parecer insuficientes en comparación a un nuevo contexto, sino también con un marco europeo muy fragmentado, dada la diversidad de modos de adaptación de cada Estado miembro.

[870] Por el contrario, el CEDH y otros Tribunales Constitucionales o superiores nacionales se han visto en la obligación de pronunciarse en situaciones ante la vulneración de derechos fundamentales en crisis de seguridad nacional desde ya hace algunas décadas. *Vid*. Rosario SERRA CRISTÓBAL (2016: 494 y ss.).

supuesto un enorme avance en el campo de protección de la esfera de los derechos a la persona, debido a las dificultades de los legisladores nacionales y, sobre todo, a nivel supranacional, de determinar una tutela normativa, si no exhaustiva, a veces también mínima a las cuestiones relevantes sobre la protección de datos de carácter personal, en la misma línea de proteger la recopilación, retención y trasferencia de datos de los ciudadanos europeos por razones de seguridad pública.

15. En los "*leading cases*" elegidos, el TJUE en materia de la salvaguardia de la privacidad con las exigencias relacionadas con la seguridad ha registrado una evolución constante a lo largo de los años, y ha precedido consistentemente todas las intervenciones de codificación por el legislador europeo que, de hecho, ha tomado de las decisiones judiciales muchos de los principios posteriormente recibidos por la legislación comunitaria[871]. En consecuencia, las amenazas a la seguridad global y el orden público, como analizaremos, han proporcionado un nuevo brío al debate jurisprudencial sobre la recopilación, la conservación y la consiguiente trasferencia de información de personas, hasta el punto de merecer un estudio en el que se pone en relación con las áreas de la política internacional y las relaciones internacionales que afectan a las relaciones entre los Estados miembros, los EE.UU. y la UE.

16. En los casos que se analizarán más adelante, la intención del Tribunal ha sido aplicar las disposiciones que impedía a los Estados afectar al núcleo esencial de los derechos protegidos por la Carta de Niza y la proporcionalidad en las medidas tomadas como fuertemente restrictivas del margen de intervención del Estado (artículo 52 de la Carta). Podría decirse que, según la jurisprudencia del TEDH, gracias a los pronunciamientos del TJUE, el "margen de apreciación del Estado" se ha reducido considerablemente, con una mayor exigencia que permite garantizar el derecho fundamental a la protección de los datos personales de manera uniforme en todos los Estados miembros de la UE.

17. Del contenido de los pronunciamientos del TJUE se derivan relevantes consecuencias prácticas no sólo para los Estados europeos, sino también en las relaciones transatlánticas UE-EU.UU., que han conllevado: a) la anulación de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de los datos personales de

[871] *Vid*. Oreste POLLICINO (2013), «Internet nella giurisprudenza delle Corti europee: prove di dialogo?», en *Forum di Quaderni Costituzionali*, núm. 1/2014, págs. 27. ISSN 2281-2113. Disponible en Internet: http://www.forumcostituzionale.it/wordpress/?p=2847 [consulta: 04 de diciembre de 2015].

tráfico telefónico y telemático, con consecuencias en la negociación y conclusión del nuevo *PNR* de la UE (sentencia 8 de abril de 2014[872] en la llamada sentencia *Digital Rights Ireland*); b) la anulación del Acuerdo "*Safe Harbour*" adoptado en 2000, sobre el intercambio de datos entre EE.UU.-UE, que ha conducido a la conclusión del nuevo Acuerdo "*Privacy Shield*" en 2016 (sentencia de 6 de octubre de 2015 o sentencia *Schrems* o *Facebook*); y c) la crítica a la legislación del Reino Unido y Suecia sobre la compatibilidad de las normativas nacionales de retención de datos, es decir, la recopilación y conservación de datos de tráfico telefónico y el posterior acceso de las autoridades nacionales, de conformidad con la legislación europea. Consecuentemente, nos referimos primariamente a la, sentencia de 21 de diciembre de 2016 o sentencia *Tele2 Sverige.*

[872] Es verdad que el 2014 fue el año de la famosa sentencia *Google Spain* que, aunque importante, no pertenecea nuestra área de estudio. Sin embargo, parece apropiado hacer una breve mención. Efectivamente, sólo un mes más tarde, el 13 de mayo de 2014, el mismo Tribunal intervino sobre el tema de la privacidad y Internet, afirmando que el gestor de un motor de búsqueda es responsable del trato de los datos personales que aparecen en las páginas web publicadas por tercero. En el caso *Google Spain* el TJUE (Gran Sala) ha sido llamado ante todo a contemperar el derecho a los ciudadanos UE a la protección de la vida privada con el interés económico subtendido a la actividad de *Google*, así como con la libertad de conseguir y difundir información, en particular en la Red. La cuestión, planteada primero frente a la Agencia Española de Protección de Datos (AEPD), después a la Audiencia Nacional y finalmente al TJUE con petición de decisión prejudicial, artículo 267 del TFUE, fue determinar si un individuo podía reclamar el derecho a la protección de datos para la supresión de información de Internet relacionados con su persona, aunque verdadera y legítimamente publicadas muchos años antes por un tercero en un periódico, ya que considera perjudicial su propagación. En la misma se ha afirmado por primera vez la existencia en el derecho comunitario del llamado "derecho al olvido". Es una pronunciación fundamental, que producirá consecuencias significativas en el individuo y sobre las actividades de las multinacionales de la Red. Pues, será posible, bajo algunas condiciones, dirigiéndose directamente al motor de búsqueda, considerado responsable del tratamiento de los datos personales, para pedir la cancelación de la lista de resultados de búsqueda, los enlaces que posponen a páginas web continentes información personales. TJUE (Gran Sala), *Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos, Mario Costeja González*, asunto C-131/12, sentencia de 13 mayo de 2014. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES#Footref* [consulta: 14 de febrero de 2016]. En doctrina, entre muchos: Giusella FINOCCHIARO (2014), «Il diritto all'oblio nel quadro dei diritti della personalità», in *Il Diritto dell'informazione e dell'informatica*, anno XXIX, fasc. 4-5, págs. 591-604. Disponible en Internet: http://www.blogstudiolegalefinocchiaro.it/wp-content/uploads/2014/11/Giusella-Finocchiaro.pdf [consulta: 02 de enero de 2016]; Rosa PASTENA (2014), «Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)», en *Associazione Italiana dei Costituzionalisti*, núm. 2, luglio, págs. 13. Disponible en Internet: http://www.osservatorioaic.it/internet-e-privacy-una-relazione-complicata-a-margine-della-sentenza-della-corte-di-giustizia-del-13-maggio-2014.html [consulta: 04 de setiembre de 2015]; Diego CÓRDOBA CASTROVERDE (2014) «El "derecho al olvido" tras la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014», en *Revista de Jurisprudencia*, núm. 1, octubre; María ÁLVAREZ CARO (2015); Lorenzo COTINO HUESO (2015), «El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal"», en *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, págs. 391-433; Ana AZURMENDI (2015), «Por un "derecho al olvido" para los europeos: aportaciones jurisprudenciales de la Sentencia del TJUE del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional de 29.12.2014», en *UNED. Revista de Derecho Político*, núm. 92, enero-abril, págs. 273-310. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/14428 [consulta: 17 de diciembre de 2015]; M.ª Begoña LÓPEZ PORTAS (2015), «La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE», en *UNED. Revista de Derecho Político*, núm. 93, mayo-agosto, págs. 143-175; Giorgio RESTA, Vincenzo ZENO-ZENCOVICH (2015), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, RomaTrE-Press, aprile, págs. 362.

18. En las tres sentencias se pone de manifiesto la relevancia del tema de la seguridad pública en relación con la privacidad, cuestión de enorme importancia en una época en la que la propia libertad se ve comprometida ante las dificultades para controlar las actividades delictivas graves, y, en particular, el terrorismo. Este contexto histórico, social y político explica que exista una especial preocupación ante el abuso de ciertas técnicas de vigilancia pública, con especial atención a determinados sistemas que son percibidos por la opinión pública como particularmente invasivos, como son aquellos destinados a la conservación masiva, opaca e indiscriminada de datos personales.

19. En fin, en estos asuntos el Tribunal de Luxemburgo pretende alcanzar en su fundamentación jurídica un equilibrio de las disposiciones de la legislación secundaria (reglamentos y directivas), con la CDFUE como punto de referencia, y tratando de alcanzar una emancipación progresiva de la jurisprudencia del TEDH como perno original, evolucionando así hacia unos parámetros propios. No cabe duda entonces de que el TJUE ha asumido una posición más propia de un tribunal constitucional[873], como consecuencia de la juridificación de la CDFUE, que de lo que en realidad es, un tribunal que verifica e interpreta el derecho en una organización internacional "*sui generis*". Dicho de otro modo, ha emprendido un camino histórico hacia la constitucionalización de los Tratados: primero, consideró indispensable la interpretación del Derecho de la Unión de modo que no contraviniese las tradiciones constitucionales de los Estados miembros; después erigió el CEDH como parámetro de interpretación y como norma vinculante; y, en la actualidad,

[873] En el año 2003 el TJUE se pronunció en dos importantes sentencias sobre cuestiones de protección de datos personales: el caso *Österreichischer Rundfunk*; y el caso *Lindqvist*. Se trata de recursos relativos a la interpretación de la Directiva 95/46/CE sobre protección de datos personales, en los que el Tribunal ha reconocido ya expresamente la existencia de un derecho a la protección de datos personales, configurando algunos de sus elementos más importantes, y haciendo suya la jurisprudencia del TEDH. En la solución de los casos sometidos a su conocimiento, el TJUE ha subordinado la injerencia en la vida privada del individuo a la satisfacción de los criterios reconocidos por el artículo 8, apartado 2, del CEDH: la medida debe ser prevista por ley, necesaria en una sociedad democrática, destinada a la realización de los objetivos legítimos de interés general y proporcionada con respecto a estos últimos. En esos casos, el TJUE ha llevado a cabo una interpretación similar a la de un tribunal constitucional, mediante su control de constitucionalidad, como, además, garante último de la proporcionalidad de las normas, no sólo con respecto al Tribunal de Estrasburgo, sino también a los tribunales constitucionales nacionales. TJUE, *Österreichischer Rundfunk*, asuntos acumulados C-465/00, C-138/01 y C-139/01, sentencia de 20 de mayo de 2003. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=48330&doclang=ES [consulta: 26 de enero de 2016]; TJUE, *Bodil Lindqvist*, asunto C-101/01, sentencia de 6 de noviembre de 2003. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9409 [consulta: 22 de enero de 2016]. *Vid*. José Luis PIÑAR MAÑAS (2003: 45-90).

declara directamente la nulidad de actos jurídicos de las instituciones europeas cuando contravienen los derechos reconocidos por la Carta[874].

20. Como se podrá comprobar, a la luz de la constante sucesión de eventos relacionados con el tema del derecho a la privacidad, no es fácil encontrar el equilibrio de los requisitos mencionados arriba, piedra angular de toda sociedad democrática, que parece destinado a influir por mucho tiempo el debate jurídico y político en las instituciones de la UE.

2. La anulación de la Directiva 2006/24/CE de conservación de datos de comunicaciones electrónicas (*data retention*): el asunto *Digital Rights Ireland*

21. En el contexto histórico actual, en la constante búsqueda del equilibrio entre protección de la intimidad de los datos personales y garantía de la seguridad pública, asume un papel fundamental el examen de la sentencia de 8 de abril de 2014 del TJUE: el caso *Digital Rights Ireland*[875]. Con esta sentencia, los jueces del Tribunal han abordado las cuestiones jurídicas relacionadas con la recogida, almacenamiento y utilización de datos sensibles de un individuo residente en la Unión Europea a través de comunicaciones telefónicas o electrónicas por parte de las autoridades de los Estados miembros, que fueron reguladas por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de

[874] Ricard MARTÍNEZ (2015), «Safe Harbor: retos para el modelo europeo de la privacidad», en *Lefebvre - El Derecho*, 19.10.2015. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/Safe-Harbor-modelo-europeo-privacidad_11_874180003.html [consulta: 08 de diciembre de 2015].

[875] Entre la abundante bibliografía sobre esta sentencia vid. Elspeth GUILD, Sergio CARRERA (2014), «The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive», en *CEPS Liberty and Security in Europe Papers*, núm. 65, may 29, págs. 17. Disponible en Internet: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901 [consulta: 10 de mayo de 2015]; Franziska BOEHM, Mark D. COLE (2014), *Data Retention after the Judgement of the Court of Juistice of the European Union*, study was provided by The Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30 june, págs. 107. Disponible en Internet: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf [consulta: 15 de mayo de 2015]; Michele MESSINA (2014), «La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità», en *Osservatorio sulla Corte di Giustizia dell'Unione europea*, núm. 2, págs. 396-401; Oreste POLLICINO (2014), «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», en *federalismi.it–Focus TMT*, núm. 3, págs. 29. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?artid=28017 [consulta: 23 de mayo de 2015]; Federico FABBRINI (2015), «Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States», en *Harvard Human Rights Journal*, vol. 28, págs. 65-95. Disponible en Internet: http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf [consulta: 11 de diciembre de 2015]; Francesco BESTAGNO (2015), «Validità e interpretazione degli atti dell'UE alla luce della Corte: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali», en *Il Diritto dell'Unione Europea*, fasc.1, págs. 25 y ss; Artemi RALLO LOMBARTE (2017).

marzo de 2006[876]. Con esta decisión, llamada también "*Data Retention*", el TJUE (Gran Sala) declaró la nulidad de dicha Directiva de 2006[877], poniendo en equilibrio las necesidades de seguridad y privacidad aplicando el principio de proporcionalidad[878].

22. La importancia que otorga el TJUE a la protección de datos personales en la UE no se limita a las relaciones entre particulares, sino que también ha afectado a las que existen entre los ciudadanos y los poderes públicos.

23. La decisión es relevante por constituir un importante paso desde el punto de vista de la protección de los derechos fundamentales en tanto es el primer caso en el que el TJUE ha anulado en su totalidad un acto de Derecho derivado por ser contrario a las disposiciones de la CDFUE. Se trata a la vez de un ejemplo singular de evaluación "estricta" de la proporcionalidad por parte del Tribunal y de un supuesto en el que una impugnación indirecta a través de los tribunales nacionales deroga una legislación de la UE por el TJUE sobre la que ya se había pronunciado.

24. La Gran Sala del Tribunal dictó sentencia en los asuntos acumulados C-293/12 y C-594/12, presentados respectivamente por el Alto Tribunal de Irlanda ("*High Court*")[879] y el

[876] DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, *Diario Oficial de la Unión Europea*, L 105, 13.4.2006, págs. 54–63. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006L0024 [consulta: 28 de mayo de 2015].

[877] TJUE (Gran Sala), *Digital Rights Ireland Ltd y Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General y Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros*, asuntos acumulados C-293/12 y C-594/12, sentencia de 8 de abril de 2014.

[878] Sandro STAIANO (2017), «Diritto alla riservatezza e potere pubblico», en *federalismi.it*, núm. 17, pág. 6.

[879] El 11 de agosto de 2006, *Digital Rights Ireland Ltd*. interpuso un recurso ante la *High Court* en el que afirmaba que era titular de un teléfono móvil que fue registrado el 3 de junio de 2006 y que utilizaba desde aquella fecha. Cuestionaba la legalidad de medidas legislativas y administrativas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas y solicitaba, en particular, al órgano jurisdiccional remitente que declare la nulidad de la Directiva 2006/24 y de la séptima parte de la Ley de Enjuiciamiento Criminal (Delitos de Terrorismo) de 2005 (*Criminal Justice (Terrorist Offences) Act 2005*), que establece que los proveedores de servicios de comunicaciones telefónicas deberán conservar los datos de tráfico y localización relativos a esas comunicaciones durante el período establecido en la ley para prevenir y detectar delitos, investigarlos y enjuiciarlos, así como para garantizar la seguridad del Estado. Al considerar que la *High Court* no puede pronunciarse sobre las cuestiones que se le plantean sobre la legislación nacional sin que se haya examinado la validez de la Directiva 2006/24, decidió suspender el procedimiento y plantear al TJUE las cuestiones prejudiciales. El presidente de *Digital Rights Ireland*, TJ McIntyre, dijo: «*These laws require telephone companies and internet service providers to spy on all customers, logging their movements, their telephone calls, their emails, and their internet access, and to store that information for up to three years. This information can then be accessed without any court order or other adequate safeguard. We believe that this is a breach of fundamental rights. We have written to the Government raising our concerns but, as they have failed to take any action, we are now forced to start legal proceedings. Accordingly, we have now launched a legal challenge to the Irish government's power to pass these laws. We say that it is contrary to the*

Tribunal Constitucional de Austria ("*Verfassungsgerichtshof*")[880], por objeto sendas peticiones de decisión prejudicial de conformidad con el artículo 267 del TFUE[881] para verificar la validez de la Directiva sobre conservación de datos (Directiva 2006/24/CE). Los Tribunales Constitucionales citados interpusieron sendas cuestiones prejudiciales ante el TJUE para examinar la adecuación de sus respectivas legislaciones nacionales que trasponían dicha Directiva de 2006 y, a su vez, la de ésta a los derechos fundamentales a la privacidad y a la protección de datos consagrados en la CDFUE (en particular, artículos 7, 8 y 11)[882].

25. El TJUE fijará su argumentación[883] siguiendo un hilo que se puede resumir en tres etapas: a) verificar la pertinencia de los artículos 7 y 8 de la CDFUE con el fin de evaluar la validez de la Directiva; b) averiguar si la misma constituye una injerencia en los derechos mencionados en los mismos artículos (7 y 8); c) y si tal interferencia puede justificarse.

26. Antes de continuar debe recordarse que ya en el 2006 el TJUE fue llamado a pronunciarse sobre la Directiva comentada, desestimando en el 2009 el recurso presentado

Irish Constitution as well as Irish and European Data Protection laws». En «DRI brings legal action over mass surveillance», en *Digital Rights Ireland*, 14 SEP 2006. Disponible en Internet: https://www.digitalrights.ie/dri-brings-legal-action-over-mass-surveillance/ [consulta: 18 de septiembre de 2017].

[880] La petición de decisión prejudicial en el asunto austriaco tiene su origen en varios recursos interpuestos ("*class action*") ante el *Verfassungsgerichtshof*, respectivamente por el Kärntner Landesregierung y los Sres. Seitlinger y Tschohl y otros 11128 demandantes que solicitan la anulación del artículo 102a de la Ley de telecomunicaciones de 2003 (*Tekommunikationsgesetz 2003*), que fue introducido por la Ley federal por la que se modifica dicha Ley de telecomunicaciones (*Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird, BGBl*. I, 27/2011) con el fin de transponer la Directiva 2006/24 en el ordenamiento jurídico austriaco. Las partes mencionadas consideraban, en particular, que el artículo 102a vulneraba el derecho fundamental de los particulares a la protección de sus datos.

[881] Sobre la cuestión prejudicial artículo 267 del TFUE, *vid*. Juan Manuel CRIADO GÁMEZ (2011), «La inadmisibilidad de la cuestión prejudicial prevista en el artículo 267 del Tratado de Funcionamiento de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 24, mayo, págs. 7-34. ISSN: 1696-6759; Juan Ignacio UGARTEMENDIA ECEIZABARRENA, Ricardo ALONSO GARCÍA (dirs.) (2014), *La cuestión prejudicial europea*, European inklings (EUi) IV, núm. 4, págs. 201. Disponible en Internet: https://carlosesposito.files.wordpress.com/2014/05/cuestion-prejudicial-europea-dig.pdf [consulta: 10 de enero de 2016]; Manuel CIENFUEGOS MATEO (2014), «La cuestión prejudicial comunitaria (Artículo 267 del Tratado de Funcionamiento de la Unión Europea)», en *Miami-Florida European Union Center of Excellence*, vol. 14, núm. 1, February, págs. 21. Disponible en Internet: http://aei.pitt.edu/63608/1/Cienfuegos_PrejudicialComunitariaEU_rev.pdf [consulta: 19 de enero de 2016].

[882] En particular, el Tribunal de Irlanda (asunto C-293/12) solicitó al TJUE que se pronuncie sobre la compatibilidad entre la Directiva y los artículos 7, 8, 10, 11 y 41 de la CDFUE, así como el artículo 21 del TFUE (apartado 18). El Tribunal de Austria (asunto C-594/12), sin embargo, solicitó una decisión prejudicial del TJUE en relación con los artículos 7, 8 y 11 de la Carta (apartado 21).

[883] El TJUE, a los objetivos de la disertación oral de la causa y su pronunciación final, decidió reunir a las dos cuestiones prejudiciales, ya que ambas estaban relacionadas en sustancia a una solicitud de examen de la validez de la Directiva 2006/24/CE, a la luz de su compatibilidad con los artículos 7, 8 y 11 de la CDFUE.

por algunos Estados miembros que denegaban la legitimidad de la base jurídica de la Directiva[884].

2.1. De la cooperación a la armonización en materia de seguridad: una aproximación a la Directiva 2006/24/CE

27. La Directiva 2006/24/CE, también conocida como Directiva "*Data Retention*"[885], sobre conservación de datos de tráfico y localización de comunicaciones electrónicas perseguía garantizar la disponibilidad de esos datos con «*fines de prevención, investigación, detección y enjuiciamiento de delitos graves*» (delincuencia organizada y el terrorismo) y, a tal fin, exigía a los Estados miembros que obligasen a las compañías de telecomunicaciones proveedoras de estos servicios a conservar los «*datos de tráfico y de localización y los* (…) *necesarios para identificar al abonado o al usuario*», pero no favorecía, sin embargo, la conservación del contenido de las comunicaciones. La justificación política de la introducción de la Directiva era que, al retener y analizar los metadatos de las telecomunicaciones, los actos de terrorismo y los delitos graves podrían detectarse, investigarse y enjuiciarse eficazmente[886]. Sin duda, la Directiva 2006/24/CE fue la respuesta jurídica de las instituciones europeas a los atentados terroristas de Madrid de 2004 y Londres de 2005[887].

---

[884] Mediante recurso, Irlanda solicitó al TJUE que se anulase la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, por no haber sido adoptada sobre la debida base jurídica. El TJUE confirmó en 2009 el fundamento jurídico de la Directiva relativa a la conservación de los datos. Sin embargo, en el apartado 57 de la sentencia, ha puesto de nuevo en duda la legalidad de la Directiva: el recurso interpuesto por Irlanda se refiere únicamente a la elección del fundamento jurídico y no a una posible violación de los derechos fundamentales derivados de la injerencia en el ejercicio del derecho a la privacidad contenido en la Directiva 2006/24. *Vid*. TJUE (Gran Sala), *Irlanda contra Parlamento Europeo y Consejo de la Unión Europea*, asunto C-301/06, sentencia de 10 de febrero de 2009.

[885] *Amplius*, Francesca E. BIGNAMI (2007a), «Privacy and Law Enforcement in the European Union: the Data Retention Directive», en *8 Chicago Journal of International Law*, págs. 233-255. Disponible en Internet: http://scholarship.law.duke.edu/faculty_scholarship/1602/ [consulta: 11 de noviembre de 2015]; Eleni KOSTA (2013), «The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection», en *SCRIPTed*, vol. 10, issue 3, October. Disponible en Internet: http://script-ed.org/?p=1163 [consulta: 10 de noviembre de 2015].

[886] La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, en su considerando 9 afirmaba que «*Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo* (…)».

[887] El Consejo Europeo empezó a contemplar nuevos instrumentos, en particular sobre la recopilación y el intercambio de información. Se dio especial prioridad a la retención de datos de tráfico de comunicaciones. EUROPEAN COUNCIL (2004), Declaration on Combating Terrorism, Brussels, 25 March 2004. Disponible en Internet: http://www.consilium.europa.eu/uedocs/cmsupload/decl-25.3.pdf [consulta: 19 de noviembre de 2015]. En primer lugar, se propuso un proyecto de Decisión marco sobre la retención de datos sobre telecomunicaciones sobre la base de los poderes de cooperación policial de la Unión. La propuesta incluía la obligación de los proveedores de servicios de telecomunicaciones de conservar los datos de tráfico de sus

28. La Directiva permitía la conservación de los datos de tráfico y localización, y de identificación del abonado o usuario para fines de detección y enjuiciamiento de delitos graves como la delincuencia organizada y el terrorismo. Por si hubiera alguna duda acerca de los motivos de su aprobación, en su artículo 1 (Objeto y ámbito) se proponía: «*armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro*». Y se aplicaba «*a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas*».

29. Entre los objetivos de la mencionada Directiva, se encontraba el armonizar a nivel europeo las obligaciones de los proveedores de «*conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro, como el terrorismo y la delincuencia organizada* (…)» (considerando 21). Aunque se presentaba como un esfuerzo de armonización, el proceso político y los considerandos de la Directiva sugieren que los objetivos reales de la Directiva estaban relacionados con la prevención del terrorismo y otros delitos graves[888]. Por lo tanto, la disciplina se centra en dos obligaciones establecidas a los proveedores: una de conservación de los datos y una de entrega a las autoridades. Los «*proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones*»[889] tuvieron que conservar por un período

usuarios telefónicos e Internet durante un período de 12-36 meses. Los datos estarían disponibles para la aplicación de la ley de acuerdo con la legislación nacional, pero también podrían haber sido solicitados por otros Estados miembros para la cooperación judicial en materia penal. La propuesta fue cuestionada por el Parlamento Europeo y las autoridades de protección de datos de la UE, por su desproporcionalidad, su falta de respeto por la privacidad y el fundamento jurídico formal del instrumento. La propuesta fue retirada. Vid. Christian DESIMONE (2010), «Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive», en *German Law Journal*, vol. 11, núm. 3, págs. 301-303. Disponible en Internet: http://www.germanlawjournal.com/volume-11-no-03/ [consulta: 23 de noviembre de 2015].

[888] Niklas VAINIO, Samuli MIETTINEN (2015), «Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States», en *International Journal of Law and Information Technology*, vol. 23, issue 3, 1. Disponible en Internet: https://doi.org/10.1093/ijlit/eav010 [consulta: 26 de noviembre de 2015].

[889] Artículo 3 (Obligación de conservar datos) de la DIRECTIVA 2006/24/CE.

de seis a veinticuatro meses, todos los datos de tráfico procesados[890]. El objeto de esta obligación no alcanzaba a los contenidos de las comunicaciones, sino sólo a la información extrínseca: el número de teléfono de llamada, el nombre y la dirección del abonado o usuario registrado, la ubicación, el número o números marcados, la identificación del llamante como del llamado y la fecha y hora de inicio y final de la conversación, así como sus análogos de informática, en particular, la dirección *IP* y los momentos de inicio y final de la conexión, tipo de comunicación (teléfono o servicio de Internet utilizado), *etc*.[891].

30. La Directiva concedió a los proveedores de servicios de comunicaciones un poder-deber de intervenir de manera desproporcionada los derechos de los ciudadanos. La obtención de los datos, de hecho, hace referencia a todos los usuarios, sin discriminación en base a la presencia de un indicio o de cualquier vínculo con un hecho criminal. La imposición fue acompañada por la concesión de gran libertad de ponderación que se atribuía a sujetos sin legitimidad; además, generaba sacrificios innecesarios de privacidad, que habrían sido previsibles y evitables sin suponer un daño a la seguridad. La única obligación del tratamiento que se aplica a los proveedores fue implementar «*medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos*»[892].

31. En este sentido, "la conservación de los datos de telecomunicaciones supone una injerencia clara en el derecho a la intimidad de las personas afectadas tal como está establecido en el artículo 8 del CEDH y el artículo 7 de la Carta"[893].

---

[890] Artículo 6 (Períodos de conservación) de la DIRECTIVA 2006/24/CE: «*Los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación*». El artículo 6, requería, en particular, a los proveedores de servicios comunicación electrónica o de una red pública de comunicaciones de retener por un largo tiempo (hasta veinticuatro meses) determinadas categorías de datos sensibles con respecto a los usuarios - para identificar la fuente de la información y el destinatario, la fecha, la hora, frecuencia y duración de una determinada comunicación telefónica o electrónica - capaces de conclusiones muy precisas sobre la vida de los usuarios, a fin de hacerlos accesibles a las autoridades nacionales competentes.

[891] *Vid*. *amplius*, artículo 5 (Categorías de datos que deben conservarse) de la DIRECTIVA 2006/24/CE.

[892] Artículo 7 (Protección y seguridad de los datos), letra b), de la DIRECTIVA 2006/24/CE.

[893] «*The retention of telecommunications data clearly constitutes an interference with the right to privacy of the persons concerned as laid down by Article 8 of the European Convention of Human Rights* (…) *and Article 7 of the EU Charter of Fundamental Rights*». *Vid*. EDPS (2011b), Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), Brussels, 31st May 2011.

32. Desde su propuesta, la Directiva 2006/24/CE fue objeto de un amplio debate[894], por su fuerte incidencia sobre los derechos fundamentales. De hecho, en el 2011 se publicó un Informe de la Comisión sobre la Directiva[895] en el que se reconocía la utilidad de la normativa en las investigaciones penales contra la delincuencia y el terrorismo, pero se indicaban deficiencias y críticas sobre el diseño de la Directiva, en particular, en relación con el equilibrio entre seguridad y privacidad[896]. Además, el Informe, por una parte, está de acuerdo con la opinión del SEPD, que señaló que la Directiva en cuestión no había alcanzado el objetivo de armonizar las leyes nacionales sobre la conservación de los datos personales, pero, por otro lado, sin embargo, se consideraba necesaria la técnica de retención de datos en la prevención y la lucha contra los delitos graves, incluido el terrorismo internacional.

[894] Tanto el SEPD como el Grupo de Trabajo expresaron sus preocupaciones por la necesidad y proporcionalidad de la propuesta: DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final], *Diario Oficial de la Unión Europea*, C 298, 29.11.2005. ARTICLE 29 DATA PROTECTION WORKING PARTY (2005), Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 1868/05/EN, WP 113, adopted on 21st October 2005. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf [consulta: 15 de noviembre de 2015]. También después de la aprobación de la Directiva, el Grupo siguió en las críticas: ARTICLE 29 DATA PROTECTION WORKING PARTY (2006), Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 654/06/EN, WP 119, adopted on 25 March 2006; Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, 00068/10/EN, WP 172, adopted on 13 July 2010. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp172_en.pdf [consulta: 18 de noviembre de 2015]. En doctrina, vid. Mònica VILASAU SOLANA (2006), «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad», en *IDP. Revista de Internet, Derecho y Política*, núm. 3, págs. 14-15. ISSN: 1699-8154. Disponible en Internet: http://www.uoc.edu/idp/3/dt/esp/vilasau.html [consulta: 30 de noviembre de 2015]; Lexi PIMENIDIS, Eleni KOSTA (2008), «The impact of the retention of traffic and location data on the internet user», en *Datenschutz und Datensicherheit - DuD*, vol. 32, issue 2, págs. 92-97; Franziska BOEHM, Mark D. COLE (2014).

[895] INFORME DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), COM/2011/0225 final, 18/04/2011. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52011DC0225 [consulta: 05 de diciembre de 2015].

[896] Del Informe se desprende: en primer lugar, que muchos tribunales constitucionales de los Estados miembros han declarado la inconstitucionalidad de las leyes nacionales de aplicación de la Directiva 2006/24/CE. De hecho, la Directiva había sido objeto de «*diversos procedimientos legales en los Estados miembros de la UE: Tribunal Constitucional Federal de Alemania (Bundesverfassungsgericht), 1 BvR 256/08, de 2 de marzo de 2010; Tribunal Constitucional Federal de Rumanía (Curtea Constituțională a României), n. 1258, de 8 de octubre de 2009; Tribunal Constitucional de la República Checa (Ústavní soud České republiky), n. 94/2011 Rec., de 22 de marzo de 2011*». En segundo lugar, en relación con la transposición de la Directiva, se subraya la falta de un enfoque común de los Estados miembros en función de los mecanismos y tratamiento de datos personales y la falta de garantía del respeto del derecho a la privacidad y la protección de datos personales en el almacenamiento de los datos.

33. La Directiva, de hecho, adoptada con el fin de armonizar la legislación de los Estados miembros sobre la conservación de los datos personales recogidos a través de servicios de comunicaciones electrónicas, muestra desde su principio dudas sobre la idoneidad de las medidas previstas en la normativa, y sobre que se puedan considerar realmente "necesarias" y "proporcionadas", como el CEDH exige en cada caso para la injerencia en el derecho a la privacidad.

34. Hecha esta breve introducción de los elementos clave de la Directiva impugnada, ahora vamos a examinar el razonamiento que llevó al TJUE a anular la Directiva "*Data Retention*".

2.2. La existencia de una injerencia especialmente grave en la privacidad y su justificación en los derechos garantizados por la Carta

35. En primer lugar, al declarar la nulidad, el TJUE indica que la conservación de los datos, objeto de la Directiva 2006/24/CE, constituye *prima facie* una injerencia en los derechos fundamentales de las personas involucradas, porque la conservación de estos datos permite llegar a conclusiones muy concretas sobre la vida privada de las personas, tales como costumbres cotidianas, lugares de residencia permanente o temporal, traslados diarios o de otro modo, actividades realizadas, relaciones sociales y medios sociales que frecuentan[897]. De hecho, aunque los artículos 1, apartado 2, y 5, apartado 2, de la Directiva 2006/24/CE, declaran que se prohíbe la conservación del contenido de las comunicaciones y la información consultada utilizando una red de comunicaciones electrónicas[898], sin embargo, estas previsiones legales podrían «*tener una incidencia en el uso por los abonados o usuarios registrados de los medios de comunicación a que se refiere esta Directiva y, en consecuencia, en el ejercicio por parte de éstos de su libertad de expresión, garantizada en el artículo 11 de la Carta*» (apartado 28).

[897] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 27. Estos datos permiten «*extraer conclusiones muy precisas sobre la vida privada de las personas*» cuyos datos han sido retenidos: pueden predecir los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los movimientos regulares. Incluso las actividades de los usuarios, sus relaciones sociales y entornos sociales se revelan. Lucia SCAFFARDI (2017), «Data retention e diritti della persona», en *Costituzionalismo.it*, fascicolo núm. 2, Saggi e articoli - Parte II, pág. 63. Disponible en Internet: http://www.costituzionalismo.it/articoli/630/ [consulta: 30 de octubre de 2017].

[898] La conservación de datos es autorizada por la Directiva, a saber, los necesarios para «*rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación, el equipo de comunicación de los usuarios y para identificar la localización del equipo de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet*». En TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 26.

36. Por consiguiente, la conservación de estos datos y, sobre todo, la posibilidad de acceso a los mismos por las autoridades nacionales competentes «*afecta de manera directa y específica a la vida privada*» de las personas, y por lo tanto, a los derechos garantizados por el artículo 7 de la CDFUE. Además, la conservación de estos datos también entra en el ámbito del artículo 8 de la Carta, en el tratamiento de los datos personales[899]. Asimismo, el Tribunal recuerda que, según jurisprudencia del TEDH[900], el mero acceso a los datos por las autoridades nacionales competentes es una «*injerencia adicional*» con los derechos garantizados por los artículos 7 y 8 de la CDFUE[901].

37. En síntesis, según el Tribunal de Justicia, por lo tanto, la injerencia de las medidas de la Directiva 2006/24/CE en relación con los derechos fundamentales establecidos en los artículos 7 y 8 de la CDFUE sería «*especialmente grave*». En efecto, como oportunamente subrayó el Abogado General Cruz Villalón en los puntos 52 y 72 de sus conclusiones, «*la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante*»[902].

38. Después de la identificación de estos parámetros, los jueces empiezan a hacer frente a la existencia de una posible violación de la privacidad y de la protección de los datos personales y creen que, de hecho, la disponibilidad de datos que gozan las empresas de comunicaciones y las autoridades nacionales competentes y la falta de información de un procesamiento masivo de datos constituyen lesiones graves de estos dos derechos. Una vez concluido que existe una injerencia, se trata de valorar la legalidad bajo las normas generales del sistema europeo.

---

[899] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 29. El Tribunal también señala que la obligación puesta a los operadores de servicios de telecomunicaciones (artículos 3 y 6 de la Directiva 2006/24/CE), de conservar los datos relativos a la vida privada de una persona y a sus comunicaciones, constituye una injerencia con el derecho al respeto de la vida privada y familiar garantizado por el artículo 7 de la CDFUE, ya que el acceso a los datos permite una información muy precisa sobre la esfera personal de los individuos involucrados (apartado 34). El TJUE entiende (apartado 33) que, «*para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia*». El Tribunal cita en apoyo su propia sentencia en el caso *Österreichischer Rundfunk y otros* de 2003. TJUE, *Österreichischer Rundfunk*, apartado 75.

[900] Véase, en lo que respecta al artículo 8 del CEDH, las siguientes sentencias ya citadas arriba en el apartado de la jurisprudencia del TEDH: *Leander contra Suecia*, apartado 48; *Rotaru contra Romania* [GS], apartado 46.

[901] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartados 35 y 36.

[902] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 37. Lucia SCAFFARDI (2017).

39. A pesar de la importancia de la justificación que supone la lucha contra las actividades terroristas y, en general, la protección de la seguridad colectiva reconocida por el TJUE como objetivo final de la Directiva de conformidad con el artículo 52 de la CDFUE, no es sin embargo posible, considerar compatible con los principios de proporcionalidad y necesidad el contenido de la Directiva[903].

40. Los mismos jueces se apresuran a señalar que, aunque son «*especialmente graves*», las lesiones producidas por la Directiva 2006/24/CE no violan la esencia de los derechos relacionados con el derecho a la vida privada (artículo 7 de la Carta)[904], puesto que la Directiva expresamente excluye la posibilidad de conservar el contenido de las comunicaciones. Del mismo modo, el TJUE afirma que tampoco el contenido esencial de los derechos en virtud del artículo 8 de la Carta se veía afectado porque el artículo 7 de la Directiva establecía expresamente el cumplimiento de principios relativos a la protección y la seguridad de los datos conservados[905] (en particular con arreglo a la Directiva 95/46/CE y Directiva 2002/58/CE), para así constatar que el objetivo principal de la Directiva es, pues, contribuir a la lucha contra la delincuencia grave y, en definitiva, a la seguridad pública (apartado 41). Desde entonces, el TJUE ha planteado el problema de evaluar si la interferencia o restricción en cuestión podrían cumplir una meta o un objetivo de interés general.

2.3. Una vigilancia constante, indiscriminada y "desproporcionada"

41. A tal efecto, el TJUE declaró que, si bien el objetivo de la Directiva 2006/24/CE era «*armonizar las disposiciones de los Estados miembros*» de la UE relativas a las obligaciones sobre la conservación de datos, el fin material de la Directiva era garantizar la disponibilidad de los datos para la investigación, comprobación y persecución de delitos graves, contribuyendo así a la lucha contra la delincuencia y, por tanto, al "mantenimiento de la seguridad pública". El TJUE recuerda que, de su jurisprudencia precedente[906] «*se desprende*

[903] En este sentido, los jueces hacen referencia al artículo 52, apartado 1, de la CDFUE, que, repetimos otra vez más, establece: «*Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás*». TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 38.

[904] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 39.

[905] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 40.

[906] Con el fin de apreciar plenamente los resultados alcanzados por el TJUE, en el intento de recurrir su más importante jurisprudencia en referencia al objeto de la investigación es conveniente analizar brevemente los términos de la controversia del más conocido caso Kadi. Yassin Abdullah Kadi es un ciudadano saudí que en 2001 se le incluyó en una lista de terroristas bajo sospecha de estar vinculado a la red terrorista de Osama Bin

que la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión» y «*lo mismo ocurre en lo que respecta a la lucha contra la delincuencia grave para garantizar la seguridad pública*»[907]. Por otra parte, en última instancia, se afirma que todas estas medidas tratan de asegurar que el derecho a la seguridad tiene un objetivo legítimo ya que el artículo 6 de la CDFUE «*establece el derecho de toda persona no sólo a la libertad, sino también a la seguridad*» (apartado 42).

42. El propósito material de la Directiva parecía cumplir el requisito de la finalidad de objetivos de interés general[908], dada la importancia de la conservación y uso de los datos contemplados en la Directiva misma, como herramientas eficaces para la prevención y lucha contra el crimen[909].

Laden. Esta inscripción se produce como resultado de un Reglamento comunitario (n. 881 de 27 de mayo de 2002), en aplicación de la Resolución n. 1390/2002 del Consejo de Seguridad de las Naciones Unidas que impuso determinadas medidas restrictivas específicas contra las personas o empresas vinculadas a *Al Qaeda*. El Reglamento fue impugnado por el Sr. Kadi ante los tribunales de la UE. El Sr. Kadi declaró que no había sido informado de los motivos de su inclusión en la lista de personas y entidades sujetas a las sanciones establecidas. Por lo tanto, no había tenido la posibilidad de presentar un recurso judicial contra dichos motivos y, en consecuencia, su derecho a ser oído, así como su derecho a la tutela judicial efectiva habían sido vulnerados. Con sentencia de 3 de septiembre de 2008, la Gran Sala del TJUE anula el Reglamento comunitario n. 881/2002 en lo que respecta a los recurrentes. El Tribunal, señalando que el Reglamento en cuestión no garantiza al individuo ninguna tutela jurisdiccional contra las medidas restrictivas y, al mismo tiempo, constituye una restricción injustificada de su derecho (de propiedad). Por lo tanto, procede considerar fundado el motivo en el que el Sr. Kadi invoca la violación de su derecho fundamental (apartado 371). La sentencia, apartado 363, reconoce que: «*Frente a un objetivo de interés general tan fundamental para la comunidad internacional como la lucha por todos los medios, de conformidad con la Carta de las Naciones Unidas, contra las amenazas que los actos de terrorismo suponen para la paz y la seguridad internacionales, la congelación de fondos, activos financieros y otros recursos económicos* (…) *no puede calificarse, en sí, de inadecuada o desproporcionada*». Este precedente, es una histórica sentencia sobre la armonización de las prácticas en Europa, entre las obligaciones de derecho internacional, que surge de las Resoluciones del Consejo de Seguridad de la ONU, y la necesidad de protección de los derechos fundamentales. Vid. TJUE (Gran Sala), *Yassin Abdullah Kadi y Al Barakaat International Foundation contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas*, asuntos acumulados C-402/05 P y C-415/05 P, sentencia de 3 de septiembre de 2008; también TJUE (Sala Tercera), *Stichting Al-Aqsa y Consejo de la Unión Europea*, asuntos acumulados C-539/10 P y C-550/10 P, sentencia de 15 de noviembre de 2012. Rosario SERRA CRISTÓBAL (2015a: 45).

[907] Véase, en este sentido, los apartados 46 y 47 de sentencia *Tsakouridis*, en TJUE (Gran Sala), *Land Baden-Württemberg y Panagiotis Tsakouridis*, asunto C-145/09, sentencia de 23 de noviembre de 2010.

[908] Aunque, como se ha indicado, el objetivo declarado de la Directiva 2006/24/CE era la armonización de las obligaciones de los prestadores de servicios en el mercado común, el Tribunal considera que su «*objetivo principal*» consiste en garantizar que los datos estén disponibles para la investigación, detección y enjuiciamiento de delito grave. La conservación de los datos contribuye a la seguridad pública. Sobre esta base, el Tribunal admite que la injerencia cumple un objetivo de interés general. TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 44. Niklas VAINIO, Samuli MIETTINEN (2015).

[909] Edoardo A. ROSSI (2015), «Recenti sviluppi in tema di diritto alla privacy e alla protezione dei dati personali nello spazio giuridico europeo», en *federalismi.it–Focus TMT*, núm. 2, págs. 42. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29632 [consulta: 27 de enero de 2016].

43. A pesar de que la conservación de los datos responde sin duda a la necesidad de garantizar la seguridad, el TJUE considera que varias circunstancias demuestran inequívocamente que las disposiciones impugnadas exceden los límites de lo que parece ser «*estrictamente necesario*» para garantizar la seguridad, y no se consideran suficientes para justificar el alcance de la injerencia en los derechos fundamentales, dando lugar a una restricción desproporcionada de esos derechos. El Tribunal llegó a la conclusión, en este caso, de que la injerencia en la vida privada de los ciudadanos de la UE, aunque permitida en principio por la Directiva, no resulta justificada al no alcanzar el objetivo de garantizar la seguridad pública. A este respecto, el TJUE recuerda que: «*el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos*» (apartado 46). El control jurisdiccional en la apreciación de la proporcionalidad incumbe al legislador, que en el presente caso tiene un margen de apreciación bastante limitado dada la importancia de la protección de los datos personales en lo que respecta al derecho fundamental al respeto de la vida privada y a la magnitud y gravedad de la injerencia en este derecho que supone la Directiva 2006/24/CE[910].

44. Sobre este punto, resulta esencial el apartado 51 de la sentencia, que establece: «*en cuanto al carácter necesario de la conservación de datos que impone la Directiva 2006/24, ha de señalarse que es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación. Sin embargo, este objetivo de interés general, por fundamental que sea, no puede por sí solo justificar que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha*». En otras palabras, el Tribunal, si bien admite la legalidad de los instrumentos de conservación de datos, señaló que las actividades de protección de los datos, como se rige por la Directiva 2006/24/CE, no constituyen medidas que se limitan al mínimo necesario para lograr el objetivo de la detección y enjuiciamiento de delitos graves, como, en particular, los delitos relacionados con el crimen organizado y el terrorismo.

[910] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartados 47 y 48.

45. La normativa de la UE de que se trata aquí, por lo tanto, tiene que "establecer reglas claras y precisas sobre el alcance y la aplicación" de las medidas de la Directiva en cuestión, mediante la imposición de garantías mínimas para las personas implicadas, cuyos datos han sido conservados y de que sean suficientemente protegidos contra el riesgo de abuso, y contra cualquier acceso o uso ilícito de esos datos[911]. En particular, según el TJUE, la conservación de todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el "acceso a Internet", el "correo electrónico por Internet y la telefonía por Internet" «(…) *es aplicable a todos los medios de comunicación electrónica, cuyo uso está muy extendido y* (…) *constituye una injerencia en los derechos fundamentales de prácticamente toda la población europea*» (apartado 56). La interferencia «*afecta con carácter global a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales. Por lo tanto, se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves*» (apartado 58).

46. El TJUE anuló la Directiva de conservación de datos precisamente porque la necesidad de retener datos personales no estaba suficientemente justificada. Dicho tratamiento de datos de personas que no son inicialmente sospechosas de un delito también ocurre con respecto a los otros instrumentos objeto de este estudio. Por ello queda por ver si la sentencia del TJUE tendrá algún impacto en la práctica. Podría ocurrir que, siguiendo la misma argumentación del asunto de la Directiva, otros instrumentos de intercambio de datos (incluidos el SIS y SIS II, el VIS, Eurodac) pudieran verse afectados en el futuro.

47. Hay que señalar, que no se encuentra en el contenido de la Directiva «*ningún criterio objetivo*», ni condiciones materiales o procesales, que garanticen el acceso a los datos sólo para perseguir delitos especialmente graves dejando a cada Estado la concreción del término «*delitos graves*» definidos por cada Estado miembro en su ordenamiento jurídico interno[912].

[911] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartados 54 y 55. Véanse, por analogía, en lo que respecta al artículo 8 del CEDH, las sentencias antes citadas del TEDH, *Rotaru contra Romania*, apartados 57 a 59, y *S. and Marper contra Reino Unido*, apartado 99.

[912] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 60. En particular, la Directiva «*no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido*». También, teniendo en cuenta estos factores, el TJUE ha movido críticas concretas sobre la Directiva: el acceso a la información sólo sería aceptable si estuviese confinado a finalidad de seguridad, y en todo caso nunca sin la supervisión de una autoridad jurisdiccional o independiente. *Vid*. TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 62. Lucia SCAFFARDI (2017: 64).

48. Otro elemento crítico según el Tribunal de Luxemburgo atañe al período de conservación de los datos. El artículo 6 de la Directiva "*Data Retention*" prescribía un período mínimo de conservación de seis meses y máximo de veinticuatro sin precisar criterios objetivos que diferencien entre categorías de datos, sobre la base de su posible mayor o menor utilidad de acuerdo con la finalidad y la categoría de las personas involucradas. Por lo tanto, se llega a la conclusión de que la determinación de la duración del período de conservación no parece basarse en un criterio objetivo que limite la duración a lo estrictamente necesario[913].

49. El Tribunal deduce que la Directiva 2006/24/CE no establece reglas claras y precisas que disciplinen la extensión de la injerencia con los derechos establecidos en los artículos 7 y 8 de la CDFUE. Se puede decir, por lo tanto, que la Directiva en cuestión constituye «*una injerencia en los derechos fundamentales de gran magnitud y especial gravedad*» en el ordenamiento jurídico de la Unión, sin que tal injerencia sea circunscrita por disposiciones que determinan precisamente lo que es estrictamente necesario para alcanzar el objetivo material de la Directiva (apartado 65). El TJUE critica al legislador europeo puesto que debe fijar límites, condiciones y controles a la compresión de los derechos. Se especifica que el sacrificio de las libertades fundamentales debe seguir los parámetros de necesidad y proporcionalidad[914].

50. Además, la Directiva no garantizaba ni que los datos se conservasen en el territorio de la Unión Europea ni el control por una autoridad independiente. Bajo este aspecto, el Tribunal cree que aparece inválida, por falta de predicciones que requieren la actuación en

[913] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartados 63 y 64. El Tribunal, sin embargo, a diferencia del Abogado General, no se detiene en detalle en la cuestión temporal, ni define en sí una duración adecuada para la conservación de los datos recogidos.

[914] Con respecto a la seguridad y la protección de los datos recogidos, la Directiva 2006/24/CE no prescribía salvaguardias adecuadas, de conformidad con el artículo 8 de la CDFUE, para garantizar la protección efectiva de esos datos contra el riesgo de abuso y el acceso y uso ilícitos de los mismos. En particular, el artículo 7 de la Directiva no establecía normas específicas que tuvieran en cuenta la gran cantidad de datos cuya conservación exigía la Directiva y la distinta sensibilidad de los datos en cuestión como ningún derecho fue concedido al titular (apartado 66). En concreto, como ha señalado por el propio TJUE, la disposición autoriza a los «*proveedores a tener en cuenta consideraciones económicas al determinar el nivel de seguridad que aplican en lo que respecta a los costes de aplicación de las medidas de seguridad*» (apartado 67). Esto representa un punto débil importante, porque la obtención de los datos creaba riesgos para la privacidad que no contribuían a la calidad de las investigaciones. Difícilmente las empresas proveedoras de servicios de comunicaciones (*providers*) se habrían cargado de gastos improductivos para tutelar la privacidad, y éstos lo hicieron por propio interés, ya que la Directiva no requería a las empresas vínculos y controles de las limitaciones en el uso de la información, y esto les permitió vender las masas de los datos o la explotación de los mismos con fines publicitarios. En última instancia, se atribuye a los proveedores la facultad de crear un daño desproporcionado en comparación con el fin: estuvo claro que las empresas sólo habrían actuado en vista de sus propios intereses y sin atención al equilibrio del sistema jurídico.

el territorio de la Unión, con el resultado de que la información pudo ser transferidaa Países que no habrían garantizado un sistema equivalente a los controles comunitarios y que puede llegar a impedir las actividades de supervisión del cumplimiento de los requisitos de protección y seguridad de una autoridad independiente, como se exige expresamente en el artículo 8, apartado 3, de la CDFUE. Dicho control, efectuado sobre la base del Derecho de la Unión, para citar las palabras propias del Tribunal, «(…) *constituye un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales*»[915]. En conclusión, las obligaciones de recogida configuradas por la Directiva habrían causado más daños adicionales a la confianza de los estrictamente necesarios. De acuerdo con el TJUE, habrían tenido que prevenir esos efectos mediante la imposición de conservación en la Unión y la predisposición de medidas de seguridad de los datos adecuados a la masa de información.

51. Las consideraciones referidas se consideran suficientes para llegar a la conclusión de que la interferencia causada por el legislador de la UE, al adoptar la Directiva 2006/24/CE, «(…) *sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta*» (apartado 69), y que, por lo tanto, incluso sin la necesidad de considerar las demás cuestiones planteadas en las cuestiones prejudiciales planteadas por los tribunales nacionales[916] (en particularmente las relativas a una posible lesión de la libertad de expresión, con respecto artículo 11 de la CDFUE), debe declarar la invalidez del acto.

52. Por lo tanto, el juez europeo no declara ilegítima la recogida de datos en sí, sino que cree desproporcionado el método con respecto del derecho fundamental en relación con el derecho fundamental a la privacidad. Así pues, una vigilancia generalizada, preventiva y el

[915] Este requisito se garantizaría, en particular, al exigir, de conformidad con el artículo 8, apartado 3, de la Carta, que «*el respeto de estas normas quedará sujeto al control de una autoridad independiente*» de los Estados miembros para controlar el uso de estos datos por las autoridades públicas. Esta supervisión por las autoridades nacionales independientes asume así un papel esencial en el razonamiento de los jueces de Luxemburgo. *Vid*. TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 68: «(…) *ha de añadirse que dicha Directiva no obliga a que los datos en cuestión se conserven en el territorio de la Unión, por lo que no puede considerarse que el control del cumplimiento de los requisitos de protección y seguridad* (…) *está plenamente garantizado por una autoridad independiente, como se exige expresamente en el artículo 8, apartado 3, de la Carta. Dicho control, efectuado sobre la base del Derecho de la Unión, constituye un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales*».

[916] Fausto VECCHIO (2014), «L'ingloriosa fine della direttiva Data Retention, la ritrovata vocazione costituzionale della Corte di Giustizia e il destino dell'art. 132 del Codice della Privacy», en *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, núm. 4, págs. 212-220. Disponible en Internet: http://www.unikore.it/index.php/indici-koreuropa/numero-4#.Vgu7N5eK-Ic [consulta: 24 de abril de 2015].

uso de datos relacionados sin las garantías mínimas descritas son incompatibles con los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, aunque persiguen objetivos de interés general, como la represión de la criminalidad.

2.4. Reacciones legislativas y judiciales en los Estados miembros después de Digital Rights Ireland

53. La sentencia *Digital Rights Ireland* constituye un punto de inflexión en el que el Tribunal de Luxemburgo toma el mando en la protección de los derechos humanos europeos, dejando atrás al Tribunal de Estrasburgo y al margen de apreciación[917]. Sin embargo, la sentencia puede tener efectos revolucionarios sólo en la medida en que los Estados miembros los sigan. Después de la sentencia, los Estados miembros han adoptado posiciones diferentes respecto de la legislación nacional que parecen corresponder a dos interpretaciones contrapuestas de la decisión de *Digital Rights Ireland*[918].

54. De acuerdo con lo que llamamos interpretación "permisiva", los principales motivos de anulación de la Directiva 2006/24/CE eran que no alcanzaba un equilibrio adecuado entre el objetivo y los medios. En este punto de vista, el problema no radicaba en la idea de conservación global, sino en su aplicación. En efecto, la Directiva regulaba el acceso, el uso y la seguridad de los datos a un nivel muy general, estableciendo únicamente requisitos vagos como «*los datos estarán sujetos a las medidas técnicas y organizativas adecuadas*» (artículo 7) o «*autoridades competentes*» (artículo 8). El uso de una formulación tan aleatoria es compatible con la interpretación de que la competencia del legislador de la Unión estaba, en el momento de redactar la Directiva, limitada a las cuestiones del primer pilar. Las disposiciones específicas relativas al acceso a los datos eran ajenas a la competencia. Se puede especular si éste fue uno de los factores que salvaron la Directiva en la sentencia de 2009[919]. Sin embargo, lo que salvó la Directiva en la era pre-Lisboa, se convirtió en su

[917] Como se ha indicado al comienzo de este capítulo, la decisión se coloca en línea con la jurisprudencia del Tribunal de Estrasburgo sobre la aplicación del artículo 8 del CEDH en los casos de recogida, almacenamiento y utilización de datos sensibles de forma natural. Véanse TEDH, *S. and Marper contra el Reino Unido,* relativamente a la compatibilidad con el artículo 8 del CEDH (vida privada y tutela de los datos personales) del sistema de recopilación, conservación y utilización de los datos sensibles en el Reino Unido. También en la sentencia *Brunet contra Francia*, el TEDH consideró, por unanimidad, que había habido una violación del artículo 8 (derecho al respeto de la vida privada y familiar) del CEDH. El caso se refería a una denuncia acerca de los detalles del Sr. Brunet registrados en una base de datos criminal después de la extinción de la acción penal en su contra. TEDH, *Brunet contra Francia*, núm. 21010/10, sentencia de 18 de septiembre de 2014. Disponible en Internet: https://hudoc.echr.coe.int/eng#{"itemid":["001-146389"]} [consulta: 29 de abril de 2015].

[918] Niklas VAINIO, Samuli MIETTINEN (2015).

[919] *Vid*. TJUE (Gran Sala), *Irlanda contra Parlamento Europeo y Consejo de la Unión Europea*.

debilidad en la era post-Lisboa. La lectura permisiva ve la falta de salvaguardias adecuadas como la razón por la cual el Tribunal anuló la Directiva. Desde esta perspectiva, las observaciones que el TJUE hace en los apartados 57 a 68 constituyen una lista de cambios que harían que la ley fuera proporcionada, pero no es una lista absoluta. Sin embargo, según el fundamento básico de la sentencia, parece ser que alguna forma de retención obligatoria de datos para luchar contra la delincuencia grave y el terrorismo podría ser compatible con la CDFUE[920].

55. De acuerdo con la interpretación "estricta", la sentencia en la práctica prohíbe la conservación indiscriminada de datos globales, al exigir que los datos conservados deban tener una conexión con la delincuencia grave y el terrorismo[921]. El apartado 58 presenta una precondición indispensable, porque es inmediatamente seguido del apartado 59 que sugiere cómo limitar proporcionalmente la retención. Parece muy improbable que el Tribunal haga una sugerencia exacta de este tipo si no considera que esta condición es crucial[922]. Tomando la justificación dada a la Directiva y la presunción de inocencia en el artículo 48 de la CDFUE, la conexión entre la persona y el delito no especificado, aún no actualizado, es tanto más difícil que se justifique una recopilación completa de datos: el Tribunal se opone claramente a la recopilación general de datos indiscriminada[923].

56. A esta altura, a nuestro juicio, parece interesante describir, por lo tanto, las implicaciones legales de la decisión para los regímenes generales de retención de datos en la Unión Europea, particularmente en las reacciones de algunos Estados miembros de la UE. Nuestro objetivo es responder a las siguientes preguntas: ¿cómo se ha recibido y entendido el fallo en los gobiernos y tribunales de los Estados miembros y qué efecto práctico ha tenido en los regímenes nacionales de vigilancia electrónica?

[920] SURVEILLE (2014), *Surveille Paper Assessing Surveillance in the Context of Preventing a Terrorist Act*, págs. 51. Disponible en Internet: https://www.justsecurity.org/wp-content/uploads/2014/10/SURVEILLE-Paper-on-a-Terrorism-Prevention.pdf [consulta: 06 de mayo de 2015].
[921] Steve PEERS (2014), «The Data Retention Judgment: The CJEU Prohibits Mass Surveillance», en *EU Law Analysis*, 8 April. Disponible en Internet: http://eulawanalysis.blogspot.fi/2014/04/the-data-retention-judgment-cjeu.html [consulta: 04 de mayo de 2015].
[922] Martin HUSOVEC (2014), «First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU», en *The Center for Internet and Society*, 28 April. Disponible en Internet: http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court [consulta: 10 de mayo de 2015].
[923] Franziska BOEHM, Mark D. COLE (2014: 36 y ss.).

57. Como resulta lógico, los tribunales nacionales siguen la lectura estricta[924] mientras que los gobiernos prefieren, obviamente, la lectura más permisiva. Los gobiernos buscan proteger la seguridad interna y procesar eficazmente los delitos revisando sus regímenes de conservación de datos. Por ejemplo, el Reino Unido, ha optado por una lectura de la sentencia según la cual la vigilancia general no es ilegal en sí misma y que puede aplicarse a nivel nacional si existen salvaguardias adecuadas[925].

58. Por su parte, el 11 de junio de 2015, el Tribunal Constitucional belga (*Cour constitutionnelle*) anuló completamente la legislación nacional por la que se aplicaba la Directiva anulada de conservación de datos[926]. La nueva ley sobre la conservación de datos se adoptó el 29 de mayo de 2016 estableciendo unos criterios para la conservación de los datos: para los delitos menores, el acceso a los datos conservados sólo puede concederse por

[924] Recordamos que algunos de los tribunales nacionales constitucionales - Bulgaria diciembre 2008, Rumania octubre de 2009, Alemania marzo de 2010, Chipre y la República Checa marzo de 2011- ya antes de la sentencia en comentario fueron llamados a pronunciarse sobre la compatibilidad de las leyes de transposición de la Directiva 2006/24/CE con los requisitos constitucionales en materia de protección de datos, ya habían declarado la inconstitucionalidad total o parcial de las leyes nacionales de aplicación de la Directiva. En este sentido, la sentencia del TJUE cumple un objetivo importante: incorpora gran parte de las críticas presentadas por los tribunales constitucionales. De hecho, dado que ninguno de estos Tribunales Constitucionales, obligados en virtud del artículo 267, apartado 3, del TFUE, nunca habían hecho con carácter prejudicial referencia al TJUE, acerca de la validez de la Directiva de la UE, que era de hecho la verdadera razón de la incompatibilidad, la sentencia en cuestión, por iniciativa de los tribunales constitucionales de Irlanda y Austria, ha entonces resuelto la variegada aplicación del acto de que se trate en la UE. El artículo 267 (antiguo artículo 234 del TCE), apartado 3, establece que: «*Cuando se plantee una cuestión* (…) *en un asunto pendiente ante un órgano jurisdiccional nacional, cuyas decisiones no sean susceptibles de ulterior recurso judicial de Derecho interno, dicho órgano estará obligado a someter la cuestión al Tribunal*». Por lo tanto, los tribunales nacionales tienen siempre la posibilidad de diferir del TJUE cuando existan dudas sobre la interpretación de las disposiciones comunes a la luz de la compatibilidad de las leyes internas. Sobre la descripción más detallada de los casos, *vid*. Eleni KOSTA (2013) y Sandro STAIANO (2017: 8 y ss.). También en EUROPEAN COMMISSION - Memo (2014), Frequently Asked Questions: The Data Retention Directive, Brussels, 8 April 2014. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-14-269_en.htm [consulta: 01 de febrero de 2016]. Desde la perspectiva del papel de los tribunales nacionales, vid. María Isabel GONZÁLEZ PASCUAL (2014), «EL TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland», en *Revista de Derecho Comunitario Europeo*, núm. 49, Madrid, septiembre/diciembre, págs. 943-971. ISSN: 1138-4026.

[925] Mismo modo de actuar, también en Suecia y Finlandia. La reciente entrada en vigor de la *Investigatory Powers Act 2016* en el Reino Unido es una nueva e importante pieza del mosaico legislativo dedicada a las medidas de seguridad contra el crimen y el terrorismo que proyectará consecuencias en otros Países europeos. Los desarrollos legislativos en torno a estos temas son cada vez más controvertidos y complejos en su realización. Importante para los fines de nuestro estudio, analizaremos, en el apartado 3 de esta investigación, las consecuencias que la decisión *Digital Rights Ireland* ha tenido también sobre la legislación sueca e inglesa, con la sentencia del TJUE *Tele2 Sverige-Watson* (*vid*. *infra*). Con respecto a la legislación inglesa, vid. *amplius* Lucia SCAFFARDI (2017).

[926] Ley de 30 de julio 2013 "de modificación de los artículos 2, 126 y 145 de la Ley de 13 de junio de 2005 relativa a las comunicaciones electrónicas y el artículo 90 decies del Código de Procedimiento Penal", en base a las mismas razones que llevaron al TJUE para anular la Directiva. *Vid*. «Rapporto 2016 dell'Osservatorio sul rispetto dei diritti fondamentali in Europa», en *Fondazione Basso*, 2016, págs. 54. En los Países Bajos, con sentencia de 11 de marzo de 2015, el *Rechtbank Den Haag* (Corte de Distrito de La Haya) anuló totalmente la ley de conservación de datos de 18 de mayo 2009 (*Wet bewaarplicht telecommunicatiegegevens*) por incumplimiento de los artículos 7 y 8 de la CDFUE.

un período máximo de 6 meses; para los delitos más graves, el acceso puede ser solicitado por 9 meses con un período máximo de 12 meses para los delitos más graves[927].

59. En Francia, el marco jurídico que define la conservación de datos se establece principalmente en el Código de Correos y Comunicaciones Electrónicas (*Code des postes et des communications électroniques – CPCE*)[928] (artículo L. 34-1) y en la Ley de 21 de junio de 2004 y su reglamento de aplicación (Decree n. 2011-219 de 25 de febrero de 2011). El *CPEC* exige un período de conservación de 12 meses. Con arreglo a la Ley de 21 de junio de 2004, los proveedores de acceso a Internet y los servicios de alojamiento de Internet deben conservar, durante un año, la información sobre la identidad de los abonados a sus servicios que contribuyen al contenido en línea, así como datos técnicos conexos. Estos datos pueden ser consultados por las autoridades judiciales en el curso de los procedimientos judiciales[929].

60. En Alemania[930], la nueva ley de retención de datos entró en vigor el 18 de diciembre de 2015[931] y obliga a los operadores de telecomunicaciones y a los *ISP* a conservar registros telefónicos de llamadas como números de teléfono, fecha y hora de las llamadas telefónicas, el contenido de los mensajes de texto y los metadatos del usuario de Internet como las direcciones *IP*, los números de puertos y la fecha/hora de acceso a Internet durante 10 semanas y los datos de localización de teléfonos móviles durante 4 semanas. Después del período respectivo, todos los datos deben eliminarse a más tardar ende una semana. La ley

[927] Jonathon LITTLE, Mauricio F. PAEZ, Elizabeth ROBERTSON, *et. al*. (2016), «The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws», en *Jones Day Publications*, august. Disponible en Internet: http://www.jonesday.com/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws-08-11-2016/ [consulta: 02 de octubre de 2016].

[928] Code des postes et des communications électroniques, Version consolidée au 26 octobre 2016. Disponible en Internet: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987 [consulta: 07 de diciembre de 2016].

[929] Jonathon LITTLE, Mauricio F. PAEZ, Elizabeth ROBERTSON, *et. al*. (2016).

[930] El Tribunal Constitucional alemán dictó sentencia de inconstitucionalidad el 2 de marzo de 2010, reclamación constitucional presentada por un grupo de 34000 denunciantes, sobre la ley nacional de aplicación de la Directiva 2006/24/CE relativa a la conservación de datos. La aplicación alemana de la Directiva fue declarada inconstitucional por el hecho de que no cumplía los requisitos del principio de proporcionalidad. El almacenamiento incondicional de datos de tráfico no era inconstitucional como tal. Lo que hizo que el Tribunal anulara la ley fue que la legislación no garantizaba ni una adecuada seguridad de los datos ni restricciones en cuanto a los fines para los cuales podrían utilizarse los datos. Las salvaguardias no cumplían los requisitos constitucionales de transparencia y protección jurídica. *Vid*. *amplius*, Katja DE VRIES, Rocco BELLANOVA & Paul DE HERT (2010), «Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention», en *CEPS 'Liberty and Security in Europe'*, págs. 12. Disponible en Internet: https://www.ceps.eu/publications/proportionality-overrides-unlimited-surveillance [consulta: 20 de octubre de 2017]; Sandro STAIANO (2017).

[931] Jonathon LITTLE, Mauricio F. PAEZ, Elizabeth ROBERTSON, *et. al*. (2016).

prohíbe estrictamente la retención de datos sobre el contenido de las comunicaciones, los datos de correo electrónico y la información relativa a las páginas web visitadas[932].

61. En España, la Ley 25/2007 de 18 de octubre de 2007[933] (Ley de Conservación de Datos - LCD), llevo a cabo la transposición de la Directiva 2006/24/CE, relativa a la conservación de datos relacionados con las comunicaciones electrónicas y las redes de comunicaciones públicas. En este sentido, la LCD recoge la doctrina establecida en pronunciamientos anteriores del Tribunal Constitucional, de modo que introduce en la norma las siguientes garantías: "en primer lugar, que los datos sobre los que se establece la obligación de conservación son exclusivamente los datos vinculados a la comunicación o transmisión (es decir, los datos de tráfico y de localización), pero sin que pueda revelarse en ningún caso su contenido (la conversación). En segundo lugar, que la cesión de tales datos exigirá, siempre, la previa autorización judicial"[934]. Como regla general, el período de retención es de 12 meses a partir de la fecha de la comunicación, pero, previa consulta con los operadores de telecomunicaciones, este período puede ser aumentado a un máximo de 2 años y reducido a un mínimo de 6 meses, tenido en cuenta los costos de almacenamiento y retención de datos.

62. En contraste con esto, en Italia nada ha cambiado, y el tiempo de retención de datos en realidad se incrementa. Italia transpuso la Directiva 2006/24/CE con el Decreto Legislativo n. 109/2008 y con algunas enmiendas al *Codice in materia di protezione dei dati personali*[935] ("*Codice della Privacy*"), en particular al artículo 132[936]. Los últimos términos de conservación han sido sustituidos –en relación con investigaciones por delitos graves

[932] Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten', 27 May 2015.
[933] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, publicado en *BOE*, núm. 251, de 19/10/2007. Disponible en Internet: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243 [consulta: 12 de octubre de 2017]. Sobre la normativa española, vid. *amplius* José Julio FERNÁNDEZ RODRÍGUEZ (2016), «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente», en *Revista Española de Derecho Constitucional*, núm. 108, págs. 111 y ss. Disponible en Internet: https://recyt.fecyt.es//index.php/REDCons/article/view/54343 [documentos consultados: 13 de octubre de 2017].
[934] Belén VIYELLA (2013), «Ley de Conservación de Datos: pros y contras de su posible modificación», en *Ecija*, 15 junio. Disponible en Internet: http://ecija.com/sala-de-prensa/ley-de-conservacion-de-datos-pros-y-contras-de-su-posible-modificacion/ [consulta: 12 de octubre de 2017].
[935] DECRETO LEGISLATIVO 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali. Disponible en Internet: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 [consulta: 13 febrero de 2016].
[936] En este sentido, *vid*. Roberto FLOR (2014), «La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?», en *Diritto Penale Contemporaneo*, núm. 2, págs. 187 y ss.

como terrorismo, asesinatos en masa, guerra civil, crimen organizado, *etc*.– por la obligación de los operadores de telecomunicaciones de retener los datos ya recogidos desde el 21 de abril de 2015 hasta 30 de junio de 2017 sin hacer ninguna distinción entre tipo de tráfico (24 meses para el tráfico telefónico, 12 meses para el tráfico telemático y 30 días para las llamadas sin respuesta). Las condiciones de conservación en virtud del artículo 132 del *Codice della Privacy* se restablecerán a partir de julio de 2017, a menos que se vuelvan a prolongar o se adopte una nueva ley. Este marco reglamentario no se ha visto afectado por el fallo del TJUE, aunque no se han producido intervenciones que, tras el pronunciamiento, hayan constatado que las disposiciones del artículo 132 son discordantes con el marco regulador europeo[937].

63. En fin, parece que nada ha cambiado: los datos seguirán siendo recogidos, guardados y utilizados para combatir la criminalidad, a menos que el mismo legislador nacional cambie la ley[938]. Sin embargo, como hemos visto, la sentencia deja a los Estados miembros la posibilidad de interpretarla según su propio criterio[939]. Por lo tanto, las observaciones anteriores plantean la cuestión de la buena fe de los Estados miembros.

64. Por otro lado, si la Directiva ha sido acogida en forma de ley nacional es necesaria una acción de análogo rango para el cambio, que probablemente será en la dirección de la eliminación o en la dirección de la aplicación de una nueva directiva, creada sobre la anterior compatible con la CDFUE. Este es el punto crítico, porque el legislador de la UE debería,

[937] Michela TRESCA (2016), «Sicurezza vs protezione dei dati: la CGUE cambia registro», en *Amministrazione in Cammino*, pág. 6.

[938] Muchos de los Estados miembros todavía no han reaccionado al fallo del TJUE de 2014. La validez del derecho nacional es competencia de los órganos jurisdiccionales nacionales en virtud de la división del trabajo del Tribunal de Justicia en sentencias prejudiciales.

[939] Algunos países, como Luxemburgo y Dinamarca, parecen estar orientados a la adaptación y mantenimiento de las legislaciones nacionales relativas al sistema de recopilación de datos. En este sentido, el Gobierno danés ha publicado un informe en el que reconoce que, en virtud del artículo 15, apartado 1, de la Directiva sobre la privacidad electrónica, la CDFUE sigue aplicándose a la Ley de retención de datos de Dinamarca, pero sostiene que no es necesario introducir cambios importantes. El Gobierno observa que, en lo que respecta al requisito de vinculación con la delincuencia, la legislación nacional es igual a la Directiva, pero otras críticas no se aplican a la aplicación danesa. Por ejemplo, Dinamarca ha restringido el uso de los datos a casos graves de delincuencia, definidos principalmente por referencia a la pena de prisión del delito que debe ser de seis años o más. Además, según el Gobierno, el período de retención se basa en criterios objetivos, ya que es un año para todos los tipos de datos y ha habido casos en que la planificación de los ataques terroristas ha tardado más de 6 meses, por lo que la duración del período es justificada. El gobierno hace hincapié en el requisito de vinculación con el crimen, porque su conclusión es que la retención general de datos como tal no es una violación de la Carta. El gobierno argumenta que el derecho interno no está en contra de la Carta por el hecho de que la legislación danesa tiene buenas salvaguardias legales contra el abuso. El gobierno ha anunciado que probablemente propondrá una revisión de la legislación de retención de datos, lo que puede conducir a nuevos requisitos de conservación. Heini JÄRVINEN (2014), «Denmark: Data Retention is here to stay despite the CJEU ruling», en *European Digital Rights (EDRi)*, 4 June. Disponible en Internet: https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling [consulta: 25 de mayo de 2016].

en el corto plazo –aunque ya estamos a casi 4 años desde la sentencia–, aprobar una nueva directiva antes de que todos los tribunales nacionales solucionen la cuestión en conformidad con la decisión del TJUE, como ya ha sucedido con los Tribunales Constitucionales de Austria[940] y Eslovenia, que suspendieron el juicio interior a la espera de la sentencia *Digital Rights Ireland Ltd*, y que, con posterioridad a esta última, han procedido a anular sus leyes.

65. El Tribunal Constitucional de Eslovenia (*Ustavno Sodišče*), en su sentencia de 3 de julio de 2014 declaró la inconstitucionalidad de los artículos 163-169 de la *Electronic Comunications Act*, que prescribió explícitamente a los proveedores de conservación de datos de tráfico en la utilización de determinados servicios de comunicación (servicios de telefonía fija y móvil, Internet y acceso al correo electrónico, servicio de telefonía a través de Internet), por violación del derecho a la protección de datos personales[941]. En esta sentencia, el Tribunal Constitucional aplicó directamente los principios expresados por el TJUE en la sentencia de 8 de abril de 2014 en vista del hecho de que los artículos derogados fueron normas nacionales de transposición de la Directiva 2006/24/CE[942].

[940] El Tribunal Constitucional austriaco reaccionó dos meses después, habiendo recibido las respuestas a su remisión. Las leyes austriacas sobre retención de datos son contrarias al derecho a la protección de datos y al derecho a la privacidad protegidos en la CDFUE y CEDH. Así, la ley nacional se declaró nula con efecto inmediato. El Tribunal Constitucional describe la retención de datos como una interferencia masiva y afirma que su admisibilidad depende de las condiciones de almacenamiento y supresión de los datos y de las medidas de seguridad que protegen el acceso a los datos. Las disposiciones impugnadas de la legislación nacional no cumplen los requisitos porque la definición de la obligación de retención es demasiado vaga y las disposiciones relativas al acceso a los datos y su eliminación no cumplen los requisitos. Aunque el Tribunal reconoce que las nuevas tecnologías de la comunicación presentan nuevos desafíos para combatir la delincuencia, también hace hincapié en que las medidas adoptadas para afrontar los desafíos deben ser proporcionales a los riesgos. Según el Tribunal, la retención de datos tal como se aplica en la legislación austriaca constituye una interferencia excesiva con el derecho a la protección de datos y el CEDH y, por consiguiente, considera que la ley es inconstitucional. Vid. Loek ESSERS (2014), «Austrian court axes data retention law following EU high court ruling», en *Network World*, Jun 27.

[941] Vid. *amplius*, Samo BARDUTZKY (2014), «The Timing of Dialogue: Slovenian Constitutional Court and the Data Retention Directive», en *Verfassungsblog*. Disponible en Internet: http://www.verfassungsblog.de/timing-dialogue-slovenian-constitutional-court-data-retention-directive/ [consulta: 03 de junio de 2016]. Por orden de 26 de septiembre de 2013, de hecho, el Tribunal Constitucional había suspendido la sentencia sobre el recurso de inconstitucionalidad de la legislación nacional relativa a la conservación de datos, creyendo tener que considerar la opinión del Tribunal de Luxemburgo sobre la Directiva el examen del procedimiento hasta la decisión del Tribunal de Justicia.

[942] El Tribunal Constitucional de la República de Eslovenia consideró que la retención de datos era desproporcionada por cuatro razones: 1) la retención general de datos constituye una violación de los derechos de una gran proporción de la población que no justificaba tales infracciones; 2) también hace imposible la comunicación anónima, lo que el Tribunal de Justicia considera particularmente problemático en determinadas situaciones, como la petición de ayuda en caso de sufrimiento mental; 3) los argumentos en favor de períodos de retención selectivos (8 meses para los datos relacionados con Internet y 14 meses para los datos relacionados con la telefonía) no se proporcionaron ni se elaboraron en los materiales legislativos; 4) el uso de datos conservados no se limitaba a delitos graves. Samo BARDUTZKY (2014); Niklas VAINIO, Samuli MIETTINEN (2015).

66. Como puede comprobarse existe cierto desacuerdo interpretativo dada la diferencia en los enfoques elegidos por los tribunales y los gobiernos. Los tribunales se consideran protectores estrictos de los derechos fundamentales, mientras que los gobiernos tienen una actitud más permisiva hacia las restricciones de los derechos fundamentales. Esta diversidad en los planteamientos se encaja desde la perspectiva de la soberanía[943]: siempre que la ley y la jurisprudencia lo permitan, los Estados miembros tienen interés en interpretar los derechos fundamentales en la forma en que les deja el margen máximo para poner en práctica sus políticas. Esta disputa por las interpretaciones también pone de manifiesto la diferencia dentro de los paradigmas de seguridad: los tribunales toman en serio la idea de que las restricciones de derechos deben limitarse a lo estrictamente necesario incluso cuando las restricciones se justifican por la seguridad, mientras que los gobiernos parecen considerar las salvaguardias legales los derechos fundamentales como un tecnicismo que debe aplicarse, pero de la manera que menos interfiera con el objetivo de la política de seguridad[944].

2.5. En búsqueda de un justo equilibrio entre certezas e incertidumbres

67. Los efectos de la sentencia se pueden resumir básicamente en dos conclusiones: a) el Tribunal intenta poner fin a un sistema de almacenamiento masivo de datos, extendido y generalizado; b) insta a la UE a replantearse el sistema de retención de datos teniendo en cuenta los derechos fundamentales consagrados en la CDFUE, en primer lugar, el derecho a la intimidad y el derecho a la protección de datos personales.

68. En este sentido, la sentencia en cuestión es bastante severa[945]. Por un lado, en efecto, los jueces de la UE han sancionado la invalidez no de algunas partes de la normativa[946] sino

[943] Como se sabe, sin embargo, la protección del derecho a la privacidad en la UE ya no es prerrogativa exclusiva de los Estados. Sólo para limitar las fuentes del derecho comunitario, es suficiente recordar que el derecho al respeto de la vida familiar y el derecho a la protección de los datos personales están garantizados por los artículos 7 y 8 de la CDFUE, al que el Tratado de Lisboa ha dado el mismo valor jurídico que los Tratados. En este contexto, los Tribunales Constitucionales estatales ya no tienen el monopolio en el control del cumplimiento de las directivas con los derechos fundamentales, como es claro, sin embargo, a partir de las más recientes sentencias de los Tribunales Constitucionales europeos sobre la Directiva 2006/24/CE, que, en lugar de adoptar directamente el juicio sobre las leyes estatales de ejecución, se dirigen a la preventiva colaboración con el TJUE. Ejemplo son las peticiones por la *High Court* de Irlanda y el Tribunal Constitucional de Austria, de hecho, antes de tomar la decisión final, han planteado una cuestión prejudicial al TJUE, con el fin de obtener una decisión sobre la compatibilidad de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo con las disposiciones de la CDFUE. Martin HUSOVEC (2014).

[944] Niklas VAINIO, Samuli MIETTINEN (2015).

[945] Serena CRESPI (2015a), «Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati», en *Rivista Italiana di Diritto Pubblico Comunitario*, anno XXV, fasc. 3-4, pág. 834. ISSN: 1121-404X.

[946] Como había ocurrido en sentencias anteriores, por ejemplo, TJUE, *Association Belge des Consommateurs Test-Achats ASBL y otros contra Conseil des ministres*, asunto C-236/09, sentencia de 1 de marzo de 2011.

de la totalidad de la Directiva. Por primera vez el TJUE declara inválida la directiva en su conjunto, a lo que se añade el hecho de que dicha invalidez se ha ordenado *ex tunc* y por el incumplimiento de la CDFUE. Por otra parte, el TJUE rechaza la propuesta del Abogado General que, en sus conclusiones, había planteado la suspensión de los efectos de la declaración de invalidez de la Directiva, para dar tiempo al legislador de la UE a tomar las medidas necesarias para remediar la invalidez comprobada.

69. Esta opción del TJUE de no suspender los efectos de la declaración de nulidad[947] a la espera de la adopción de las medidas necesarias para dar cumplimiento a la sentencia a las instituciones que emitieron el acto anulado[948], demuestra, una vez más, la posición de los jueces europeos que consideran particularmente grave la violación de los derechos fundamentales y, en particular, de la protección de datos de carácter personal.

70. De nuevo, en contraste con los argumentos del Abogado General, los jueces de la UE no han considerado, por lo tanto, suficiente el argumento de que los Estados miembros estaban generalmente ejercidos en las facultades de moderación de investigación que les confiere dicha Directiva o que a la invalidez de este última se pudiera poner remedio en el ámbito de las medidas de transposición. En efecto, el Tribunal, mediante la anulación de la Directiva con efectos retroactivos (*ex tunc*), obliga al legislador de la Unión (Consejo y Parlamento) a replantear todo el sistema en acto, también con algunas indicaciones positivas, por ejemplo, la introducción de límites y procedimientos para la recopilación, almacenamiento y uso de los datos personales, incluidos los requisitos específicos para garantizar su conservación en la Unión y, por lo tanto, de conformidad con la legislación de la UE.

71. En atención al objeto de la presente investigación de esta sentencia puede concluirse que, conforme a la jurisprudencia del Tribunal de Estrasburgo, la conservación de los datos personales constituye una injerencia en la vida privada de las personas, independientemente

[947] La elección, especialmente rigurosa y poco frecuente en la práctica, de no hacer la salva a los efectos definitivos ya producidos por la Directiva y, por tanto, no usar una facultad que permita, desde hace tiempo, por la jurisprudencia plantear cuestiones con carácter prejudicial mediante la aplicación analógica del artículo 264 del TFUE (antiguo artículo 231 TCE), «*si el recurso fuere fundado, el Tribunal de Justicia de la Unión Europea declarará nulo y sin valor ni efecto alguno el acto impugnado. Sin embargo, el Tribunal indicará, si lo estima necesario, aquellos efectos del acto declarado nulo que deban ser considerados como definitivos*».

[948] De conformidad con el artículo 266, apartado 1, del TFUE (antiguo artículo 233 TCE), «*la institución, órgano u organismo del que emane el acto anulado, o cuya abstención haya sido declarada contraria a los Tratados, estarán obligados a adoptar las medidas necesarias para la ejecución de la sentencia del Tribunal de Justicia de la Unión Europea*».

de su posterior uso. Y para que pueda resultar admisible, de conformidad con el artículo 8 del CEDH, estas medidas deben ser dispuesta en una ley y ser necesaria en una sociedad democrática, con el respeto del principio de proporcionalidad. De hecho, la sentencia del Tribunal se basa en su evaluación de conformidad con el principio de proporcionalidad entre los medios de conservación de datos y el objetivo perseguido por el legislador de la UE a través de la adopción de la Directiva de 2006.

72. Sin embargo, la Directiva fue declarada nula porque violaba el derecho al respeto de la vida privada y familiar y autorizaba una incidencia excesiva y, por lo tanto ilegal, en el derecho a la protección de datos personales. Se informa de que, en realidad, el efecto en la práctica apreciable de la sentencia del TJUE, por un lado, es mucho menos de lo que se pueda imaginar y, por otro lado, no parece que pueda afectar significativamente el problema de la protección de la confidencialidad de la información personal de la mayoría de los usuarios.

73. En todo caso, la sentencia no ofrece herramientas suficientemente concretas para llegar a un punto de armonía entre las exigencias de seguridad colectiva y los derechos individuales. Así, se asiste a medidas, como la declaración de nulidad de la Directiva 2006/24/CE, destinada a reafirmar la necesidad de proteger el derecho a la protección de los datos personales de los individuos, pero, también, hay que hacer frente a las diferencias en la legislación entre EE.UU. y la UE, debidas a un equilibrio diferente entre las razones de seguridad, que empujan a tratos de datos cada vez más amplios y extensos, y las garantías individuales[949].

74. En definitiva, el principio que se deriva de la sentencia *Digital Rights Ireland* es que cualquier excepción a la regla general de confidencialidad de los datos se debe establecer de forma clara, precisa y previsible, y produce efectos también en cualquier otro acto de la UE y acuerdo internacional adoptado con el fin de luchar contra el terrorismo y el crimen que permita a las autoridades extraeuropeas acceder y usar los datos personales de ciudadanos UE. Corresponde, en estos casos, a las instituciones europeas evaluar si estos últimos son de conformidad con los artículos 7 y 8 de la CDFUE según la interpretación del TJUE.

[949] En Anna Lucia VALVO (2014), «La Corte di Giustizia dichiara l'invaliditá della direttiva sulla conservazione dei dati», en *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, núm. 4. Disponible en Internet: http://www.unikore.it/index.php/indici-koreuropa/numero-4#.Vgu7N5eK-Ic [consulta: 24 de abril de 2015].

75. En este caso, resulta interesante ver hasta qué punto las instituciones de la Unión desarrollarán respuestas para evaluar y cuestionar las prácticas nacionales que siguen siendo problemáticas[950].

76. A este respecto, cabe señalar una cosa muy rara: la Directiva sobre conservación de datos, declarada nula por el TJUE en 2014, aún no ha sido sustituida. El silencio de las instituciones europeas en un asunto tan importante y delicado es ensordecedor.

77. Tras la decisión del Tribunal, el legislador de la UE y los legisladores nacionales deberán corregir los elementos de incompatibilidad con la Carta. La Comisión Europea debería, por tanto, presentar una propuesta legislativa que establezca un justo equilibrio entre los intereses legítimos en juego, que tendrá en cuenta, las directrices emitidas por el TJUE en su sentencia[951].

78. A falta de una legislación específica sobre retención de datos, ésta está permitida como excepción a la privacidad de los datos de telecomunicaciones en virtud de la Directiva 2002/58/CE (Directiva sobre privacidad y comunicaciones electrónicas), como medida preventiva, pero debe ser únicamente para el propósito de luchar contra el crimen grave[952].

---

[950] El Consejo de la Unión Europea ha considerado los efectos de la sentencia en un dictamen. En primer lugar, el dictamen señalaba que el TJUE no se contentará con una evaluación estricta de la proporcionalidad y de la necesidad de medidas que constituyan graves restricciones a los derechos fundamentales, por legítimos que sean los objetivos perseguidos por el legislador de la UE: «*It confirms that the Court of Justice will not satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, however legitimate the objectives pursued by the EU legislature*». En segundo lugar, las medidas de retención no tienen ninguna posibilidad seria de aprobar la prueba de legalidad a menos que estén acompañadas de salvaguardias adecuadas: «*It also indicates that such measures do not stand a serious chance of passing the legality test unless they are accompanied by adequate safeguards in order to ensure that any serious restriction of fundamental rights is circumscribed to what is strictly necessary and is decided in the framework of guarantees forming part of Union legislation instead of being left to the legislation of Member States*». En COUNCIL OF THE EUROPEAN UNION (2014a), Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 9009/14, Brussels, 5 May 2014, págs. 8. Disponible en Internet: http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf [consulta: 27 de abril de 2015]. Este dictamen en principio quedó limitado en línea con su difusión. Finalmente, también fue oficialmente publicado en casi su totalidad, pero el documento no está disponible en el sitio web del Consejo. Un elemento más del Consejo sigue fuera del dominio público. Vid. Elspeth GUILD, Sergio CARRERA (2014: 10 y ss.).

[951] La Comisión Europea sigue subrayando la importancia "crucial" de los datos de telecomunicaciones y examinará las mejores opciones para avanzar en la conservación de los datos de telecomunicaciones, teniendo en cuenta todas las consideraciones para crear una política que garantice al mismo tiempo el pleno respeto del derecho a la intimidad y a la protección de los datos personales, la seguridad de los ciudadanos y el buen funcionamiento del mercado interior. EUROPEAN COMMISSION - Speech (2014), Exchange of Views between Commissioner Dimitris Avramopoulos and MEPs at the LIBE Committee in the European Parliament, 03 December 2014. Disponible en Internet: http://europa.eu/rapid/press-release_SPEECH-14-2351_en.htm [consulta: 02 de mayo de 2015].

[952] Sin duda, esta sentencia no sólo se recogió al reflexionar sobre el importante *vulnus* que afectaba a un derecho fundamental, sino también con la esperanza de que el legislador europeo interviniera lo antes posible sobre el asunto, lo que todavía no ha sucedido. De hecho, se ha abierto un vacío normativo en Europa en tanto

Tal retención debe limitarse a lo estrictamente necesario con respecto a las categorías de datos retenidos, los medios de comunicación afectados, las personas afectadas y la duración elegida de la retención. "Las autoridades nacionales pueden tener acceso a los datos retenidos en condiciones estrictas", incluida la revisión previa por parte de una autoridad independiente. Los datos deben conservarse dentro de la UE.

79. En este sentido, en enero de 2017, la Comisión Europea publicó una propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas, cuyo objetivo es derogar y sustituir la Directiva 2002/58/CE. La propuesta no incluye ninguna disposición específica sobre retención de datos. Sin embargo, establece que los Estados miembros pueden restringir determinadas obligaciones y derechos en virtud del Reglamento por ley, "cuando dicha restricción constituya una medida necesaria y proporcionada para salvaguardar intereses públicos específicos", incluida la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales. Por lo tanto, los Estados miembros podrían mantener o crear marcos nacionales de conservación de datos que prevean medidas de retención específicas, en la medida en que dichos marcos cumplan con el Derecho de la Unión, teniendo en cuenta la jurisprudencia del TJUE sobre la interpretación de Directiva *e-Privacy* (*vid. infra* en este mismo Capítulo la sentencia *Tele2 Sverige*) y la CDFUE. En el momento de la redacción de la investigación, las discusiones sobre la adopción del reglamento están en curso.

80. Finalmente, una cuestión planteada después de la sentencia es: ¿en qué medida es posible ejercer una vigilancia masiva y, al mismo tiempo, cumplir las garantías básicas de la CDFUE? A tenor del contenido de la sentencia la respuesta es que, esta alternativa no es posible. Por lo tanto, la sentencia del TJUE ha dado lugar a un marco impreciso y poco claro[953], lo que requeriría una intervención de las instituciones europeas que diera lugar a la

que la legislación nacional de aplicación de la Directiva 2006/24/CE se puede considerar contraria al Derecho de la Unión Europea, los ciudadanos podrían acudir a los tribunales nacionales para garantizar la plena efectividad de su protección jurídica. Obviamente, queda al margen la autonomía para la aprobación de nuevas leyes sobre el tema que se ajusten al principio de proporcionalidad y a la luz de la anterior Directiva 2002/58/CE que permite, en su artículo 15, apartado 1, excepciones a la prohibición general de conservación de datos para salvaguardar la seguridad nacional o detectar delitos (*vid. infra* sentencia *Tele2 Sverige*). Cabe recordar que ni el Reglamento 2016/679/UE (RGPD) ni la Directiva 2016/680 (que se examinarán con más detalle en el próximo Capítulo) abordan la cuestión del tratamiento de los datos personales con finalidad de prevención de los delitos de terrorismo o más generalmente a delitos graves. *Amplius* Federico FABBRINI (2015: 88).

[953] Inmediatamente después de la decisión del TJUE, el SEPD ha acogido con satisfacción la sentencia como un hito para las limitaciones de vigilancia digital de los gobiernos, pero pidiendo una nueva Directiva para prevenir que los Estados introduzcan normas en la legislación nacional con las mismas incertidumbres de la Directiva anulada. EDPS (2014), Press Statement: The CJEU rules that Data Retention Directive is invalid, 8

introducción de un nuevo sistema de retención de datos dentro del respeto a los derechos fundamentales. Las futuras decisiones que serán adoptadas a nivel europeo de reforma de conservación de datos, deberán cumplir con las siguientes exigencias: definir delitos específicos para lo que se permite la recopilación de datos personales; proporcionar la orientación sobre las medidas técnicas y organizativas para el acceso y utilización de dichos datos; procedimientos claros para el acceso a los datos de tráfico por parte de las autoridades nacionales que deben cumplir con las características de trazabilidad y seguridad; prever un control de parte de los jueces o de las autoridades administrativas independientes; prever la duración de la conservación de datos diferenciados en función de la gravedad de los delitos.

81. En vista de lo anterior, es posible concluir que el contenido de la sentencia del TJUE no se ha limitado a la propia Directiva, sino que tiene un reflejo inevitable también en cuestiones próxima a la misma, relacionadas con el almacenamiento y la transferencia de datos a la luz de la seguridad nacional y la lucha contra el terrorismo y el crimen. En este sentido, las repercusiones de la sentencia no se limitan a la UE, sino que también tienen consecuencias prácticas en la relación transatlántica con EE.UU., cuestión a la que se dedica el siguiente apartado.

2.6. Las relevantes consecuencias prácticas de la sentencia: el Passenger Name Record

82. Muchos acuerdos entre la UE y los EE.UU. que afectan a la transmisión de datos personales han sido fuertemente criticados por las autoridades europeas de protección de datos, ya que se considera que no son capaces de garantizar el cumplimiento de los principios de la UE en materia de protección de la información personal. Así ocurre con los acuerdos para regular, tanto el tratamiento y la transmisión de datos del registro de nombres de pasajeros aéreos (*Passenger Name Record - PNR*) al Departamento de Seguridad Nacional (*DHS*) de EE.UU., como la transmisión de datos bancarios y financieros a través del sistema *SWIFT* (*Society for Worldwide Interbank Financial Telecommunication*) por la UE a los EE.UU. para los fines del programa de control de las transacciones financieras de los

Apr 2014. Disponible en Internet: https://edps.europa.eu/press-publications/press-news/press-releases/2014/press-statement-cjeu-rules-data-retention_en [consulta: 03 de mayo de 2015]. Así como el Grupo de Trabajo expresaba satisfacción por la decisión del TJUE sobre la Directiva de 2006, también se ocupa de la relación entre los requisitos de privacidad y seguridad nacional bajo el ángulo particular de visión de la relación entre la UE y EE.UU. en el campo de intercambio y almacenamiento de datos personales, y se enfrenta a la necesidad de poner remedio a nivel europeo al vacío jurídico determinado por la anulación de la Directiva sobre la retención de datos. ARTICLE 29 DATA PROTECTION WORKING PARTY (2014a), Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN, WP 215, Adopted on 10 April 2014. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf [consulta: 04 de mayo de 2015].

terroristas (*TFTP*)[954] y la transferencia de datos personales desde países miembros de la UE hacia EE.UU. bajo el Acuerdo de "Puerto Seguro" (ver *infra*).

83. Los acuerdos internacionales se justifican por las razones de seguridad y prevención del terrorismo que han llevado a la UE y, sobre todo, a los EE.UU., a adoptar una serie de iniciativas legislativas en desarrollo de lo que se ha denominado "guerra contra el terror" y entre las que se encuentran medidas de conservación generalizada de los datos personales no muy diferente a la citada Directiva 2006/24/CE anulada por el TJUE, que han determinado un significativo aumento de los poderes de vigilancia electrónica de los gobiernos, dando prioridad a la necesidad de la seguridad pública sobre la de la tutela de la vida privada.

84. Entre las medidas más destacadas para satisfacer las demandas de aumento del nivel general de seguridad, se encuentra el establecimiento de bases de datos para la recogida de los datos personales en los registros de nombres de pasajeros, incluso dentro del territorio de la UE[955]. Por lo tanto, como se tuvo ocasión de comprobar en el Capítulo precedente, "el intercambio de datos personales entre las autoridades policiales en los Estados miembros de la UE se ha convertido en un elemento esencial de la cooperación internacional contra el terrorismo y la delincuencia organizada"[956]. De hecho, la Unión Europea tiene firmados numerosos acuerdos internacionales sobre el tratamiento y cesión de los datos personales del pasajero, con el fin de regular el flujo de estos datos e identificar los peligros a la seguridad colectiva. En concreto, la Unión Europea está vinculada por los acuerdos internacionales sobre la transferencia y tratamiento de dichos datos con los Estados Unidos, Australia[957] y

[954] «*Tras la aprobación de la Resolución del Parlamento de 8 de julio de 2010, el Acuerdo TFTP entró en vigor en agosto de 2010. En julio de 2011, la Comisión adoptó una Comunicación sobre las principales opciones para el establecimiento de un sistema europeo de seguimiento de la financiación del terrorismo (TFTS), sobre el que el Parlamento manifestó sus dudas. En noviembre de 2013, la Comisión anunció su intención de no presentar por ahora una propuesta de TFTS europeo*». Kristiina MILT (2019).

[955] En 2011, cuando la Comisión propuso a Unión Europea la Directiva *PNR*, sólo el Reino Unido tenía un sistema de recogida de datos *PNR* de pleno derecho.

[956] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, An area of freedom, security and justice serving the citizen, (COM(2009)0262 final), Brussels, 10.6.2009. Disponible en Internet: https://ec.europa.eu/anti-trafficking/eu-policy/communication-commission-european-parliament-and-council-area-freedom-security-and-justice_en [consulta: 11 de mayo de 2015].

[957] ACUERDO entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, *Diario Oficial de la Unión Europea*, L 186, 14/07/2012, págs. 4–16. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22012A0714(01) [consulta: 11 de mayo de 2015].

Canadá[958]. También, el 14 de julio de 2015, se iniciaron formalmente las negociaciones de un acuerdo de transferencia de datos *PNR* entre la UE y México.

85. El registro de nombres de pasajeros (en inglés, *PNR - Passenger Name Records*) «*contiene toda la información necesaria de cada viajero para la tramitación, reserva y el control por parte de las compañías aéreas*». El registro, además de los datos propios del viaje (fechas, itinerario, datos del billete, número de asiento, equipaje), «*elabora una base de datos con información personal, tales como el nombre, apellido, número de pasaporte o documento nacional de identidad, número de teléfono, dirección, información de carácter financiero, como la forma de pago y el número de tarjeta con la que se realizó la reserva*»[959].

86. El *PNR*, al contrario que las demás medidas europeas para garantizar el ELSJ, tales como el Sistema de Información de Schengen (SIS I y SIS II), y el Sistema de Información de Visados (VIS), permite a las autoridades responsables de la lucha contra el terrorismo identificar y analizar a los sospechosos desconocidos. El análisis de los datos *PNR*, pues, permitiría identificar a las personas sospechosas de haber participado en actos de terrorismo o delito grave, y que pudieran ser luego objeto de un ulterior examen de parte de la competente autoridad.

87. Dentro de estos instrumentos de control, por razón de su importancia, destaca el Acuerdo entre la Unión y los EE.UU. sobre el tratamiento y la transmisión de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los EE.UU. y la utilización de datos *PNR* para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves en la UE (*PNR* de la UE), sobre el que se va a centrar nuestra análisis a continuación.

---

[958] *Vid. infra*.

[959] Joan Lluís PÉREZ FRANCESCH, Tomás GIL MÁRQUEZ, Alejandro GACITÚA ESPÓSITO (2011), «Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?», en *Institut de Ciències Polítiques i Socials (ICPS)*, WP núm. 297, pág. 3. Disponible en Internet: https://ddd.uab.cat/pub/worpap/2011/hdl_2072_152109/ICPS297.pdf [consulta: 18 de mayo de 2015]. «*La información recopilada debe contener todo el historial de cambios de los datos de PNR y los datos recogidos en el sistema de información anticipada sobre los pasajeros (sistema API)*». También, *vid*. CONSEJO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA (2017), Reglamentación del uso de los datos del registro de nombres de pasajeros (PNR). Disponible en Internet: http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/ [consulta: 20 de octubre de 2017]; Marco BOTTA, Mario VIOLA DE AZEVEDO CUNHA (2010), «La protezione dei dati personali nelle Relazioni tra UE e USA, le negoziazioni sul trasferimento del PNR», en *Il diritto dell'informazione e dell'informatica*, anno XXVI, fasc. 2, págs. 315-341.

2.6.1. Protección de datos personales en las relaciones UE-EE.UU.: la transferencia de PNR

88. Como es bien sabido, a raíz de los atentados terroristas del 11 de septiembre de 2001, los EE.UU. adoptaron la Ley Patriota (*Patriot Act*) por la cual las compañías aéreas que operen rutas con destino u origen a EE.UU. o atraviesen su territorio deben facilitar a las autoridades estadounidenses el acceso electrónico a toda una serie de datos contenidos en sus sistemas de reservas y de control de salidas, denominado *Passenger Name Records* (*PNR*)[960].

89. A partir de la adopción del *PNR*, la Comisión Europea, al tratarse de un mecanismo cuya incidencia en los datos personales de los viajeros podría suponer la vulneración de las normas europeas y de los Estados miembros en materia de protección de datos[961], decidió iniciar negociaciones con las autoridades americanas con vistas a minimizar sus efectos. En el 18 de febrero de 2003, la Comisión Europea y la Oficina de Aduanas y Protección Fronteriza de EE.UU. emitieron un comunicado conjunto mediante el cual la Comisión autorizó temporalmente a las compañías aéreas europeas a transferir datos *PNR* a las autoridades de EE.UU., a la espera de una solución permanente al problema[962]. Estas

[960] El 19 de noviembre 2001 el Congreso de EE.UU. aprobó una nueva ley, la *Aviation and Transportation Security Act*, que requiere que todas las compañías aéreas que vuelan a EE.UU. proporcionen datos sobre sus pasajeros a la Oficina de Aduanas y Protección Fronteriza de EE.UU. (*U.S. Customs and Border Protection - CBP*) antes de que el avión despegue a los EE.UU. *Vid*. Aviation and Transportation Security Act, Public Law 107–71, 107th Congress, nov. 19, 2001. En este contexto las líneas aéreas europeas se encontraron bajo "fuego cruzado". Por un lado, la solicitud de las autoridades estadounidenses de proporcionar datos personales de sus pasajeros, en casos de incumplimiento de los requisitos por parte de las líneas aéreas europeas también podría dar lugar a una prohibición de aterrizaje en los EE.UU. para esas empresas; y, por otra parte, la legislación de la UE, que prohíbe categóricamente esa transferencia. Los datos recogidos con fines comerciales entran en el ámbito de aplicación de la Directiva 95/46/CE, lo que prohíbe la transferencia de datos a terceros Países que no garanticen un nivel adecuado de protección.

[961] Se refieren, en particular, a la Directiva 95/46/CE, y al REGLAMENTO (CEE) N. 2299/89 DEL CONSEJO, de 24 de julio de 1989, por el que se establece un código de conducta para los sistemas informatizados de reserva, *Diario Oficial de la Unión Europea*, L 220, 29.7.1989, págs. 1–7. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31989R2299 [consulta: 16 de mayo de 2015].

[962] Giovanni SARTOR, Mario VIOLA DE AZEVEDO CUNHA (2016), «Il caso Google e i rapporti regolatori USA/EU», en Giorgio RESTA e Vincenzo ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, RomaTrE-Press, pág. 109. En el mismo año, el Grupo de Trabajo del artículo 29, manifestó sus dudas y preocupaciones sobre el nivel de protección de datos, posiblemente administrado por EE.UU., e invitaba a la Comisión Europea a entablar negociaciones con las autoridades de EE.UU. para remediar a la situación y llegar a un acuerdo entre los EE.UU. y la UE, de conformidad con la legislación comunitaria sobre la privacidad, con especial referencia a las disposiciones relativas a la transferencia de datos a terceros Países. ARTICLE 29 DATA PROTECTION WORKING PARTY (2003), Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 11070/03/EN, WP 78, Adopted on 13 June 2003. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp78_en.pdf [consulta: 16 de mayo de 2015]. El dictamen del Grupo consideró excesiva la cantidad de datos que debían transmitirse, de conformidad con el artículo 6, apartado 1, letra c), de la Directiva 95/46/CE, por lo que el envío de datos debe limitarse a sólo unos pocos puntos del *PNR* y no a éste en su totalidad. En particular, debía prohibirse el tratamiento de los datos sensibles, protegidos por el artículo 8 de la Directiva. Además, la transferencia no se consideraba compatible con el fin original de la recopilación. A esto se añadia que el período de 7 a 8 años

negociaciones culminaron en mayo de 2004, con la Decisión 2004/535/CE, por la que la Comisión Europea declaraba que el nivel de protección de datos que otorgarían las autoridades americanas a los datos que le fueran transmitidos era considerado adecuado desde el punto de vista de la normativa europea, requisito indispensable a la hora de realizar transmisiones de datos a terceros países[963]. Con objeto de otorgar una base jurídica a las transmisiones de datos por parte de las compañías aéreas, el Consejo de la Unión Europea aprobó al respecto, con Decisión 2004/496/CE, la celebración de un Acuerdo entre la Comunidad Europea y EE.UU. que entró en vigor el 28 de mayo de 2004 con una vigencia inicial de tres años y seis meses[964]. Desde ese momento, las autoridades estadounidenses tenían acceso a un total de 34 datos de los pasajeros entre los que figuran referencias como nombre, dirección, forma de pago y teléfonos.

90. Los primeros aspectos problemáticos relacionados con dichos Acuerdos se han producido desde 2004, fecha del primer Acuerdo entre UE-EE.UU., por lo que respecta a la compatibilidad de los Acuerdos con normativa de derechos humanos vigentes en el espacio

para el que se almacenan los datos era considerado demasiado largo, pues sólo debían conservarse durante un período corto que no debía exceder algunas semanas o incluso meses después de la entrada a los EE.UU. En cuanto a la transferencia de datos, el único que respeta la Directiva es el sistema "*push*", en el que las compañías aéreas proporcionan a las autoridades estadounidenses los datos que necesitan. El uso de datos tampoco resultaba claro: estos debían usarse para combatir los actos de terrorismo y no debían extenderse a otros delitos graves. Posteriormente, el 29 de enero de 2004 el Grupo de Trabajo reiteró su opinión negativa y la presencia de puntos críticos en la transferencia de los *PNR* a los EE.UU. ARTICLE 29 DATA PROTECTION WORKING PARTY (2004), Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, WP 87, Adopted on 29 January 2004. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp87_en.pdf [consulta: 16 de mayo de 2015]. Con esta opinión, el Grupo de Trabajo reafirmó en primer lugar el principio de finalidad, por lo que los *PNR* sólo pueden utilizarse para combatir el terrorismo y no pueden utilizarse ni para otros sistemas como el CAPPS II ni para cualquier otro sistema capaz de realizar operaciones masivas de tratamiento de datos. De hecho, estos sistemas son cualitativamente diferentes de la simple transferencia de datos de pasajeros *PNR* e implican cuestiones de amplio alcance que deberían aclararse y en consideración de los efectos más generalizados que afectarían a los derechos fundamentales de los datos los sujetos interesados. Un segundo punto es el principio de proporcionalidad, que prohíbe la recopilación de información excesiva y no pertinente. Luego se subrayó una vez más la importancia de que la conservación se conceda por un período limitado de tiempo. Otro punto fue la prohibición de tratar datos sensibles. Por último, debería existir un ejercicio de los derechos de los interesados: se debería dar a los pasajeros información clara sobre quién utilizará los datos recopilados y para qué fines.

[963] DECISIÓN DE LA COMISIÓN de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*) *[notificada con el número C(2004) 1914]*, (Texto pertinente a efectos del EEE), (2004/535/CE), *Diario Oficial de la Unión Europea*, L 235, 6.7.2004.

[964] DECISIÓN DEL CONSEJO de 17 de mayo de 2004 relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (2004/496/CE), *Diario Oficial de la Unión Europea*, L 183/83, 20.5.2004. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOL_2004_183_R_0083_01 [consulta: 22 de mayo de 2015].

jurídico europeo. En efecto, este tipo de medidas ha dado lugar en los últimos años a problemas en relación con la posible incompatibilidad con las normas del derecho internacional de proteger el derecho a la privacidad y protección de datos personales[965].En todo caso, y a pesar de las garantías establecidas para los datos personales, sobre todo en relación con el tratamiento y cesión de los datos contenidos en el *PNR*, la principal dificultad surgía de la incompatibilidad de los acuerdos celebrados por la UE con la normativa propia de la Unión Europea.

91. Como ya se ha indicado con anterioridad, gran parte de los debates acerca de la aplicación de las disposiciones sobre protección de datos en la Unión Europea giran en torno a la necesidad o no de respetar los principios de la normativa europea en la adopción de "medidas dirigidas a garantizar la seguridad y combatir el terrorismo y la delincuencia organizada"[966]. De hecho, "la jurisprudencia del TJUE se ha basado en el delicado equilibrio entre el respeto a la privacidad y la garantía de la seguridad para decidir sobre la legalidad de la legislación europea". Así lo hizo en el 2006, cuando el TJUE se pronunció sobre el recurso presentado por el Parlamento Europeo sobre la compartición de datos personales de los usuarios de líneas aéreas en el asunto *PNR*[967]. El TJUE anuló tanto la Decisión del Consejo 2004/496/CE que autorizaba la firma de un tratado con los EE.UU. para que las compañías aéreas europeas le trasfirieran los datos personales de sus viajeros, como la Decisión de la Comisión Europea 2004/535/CE que consideraba que, en ese proceso, los EE.UU. protegían los datos de manera adecuada[968].

92. En sus explicaciones el TJUE señaló que «*el artículo 3, apartado 2, primer guión, de la Directiva excluye de su ámbito de aplicación el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, y, en cualquier caso, el tratamiento de datos que tenga por*

[965] *Vid*. *supra* artículo 17 del PIDCP, hecho en Nueva York el 19 de diciembre de 1966.
[966] En este sentido, *vid*. el trabajo de Rosario SERRA CRISTÓBAL (2016), que analiza muy bien el tema.
[967] TJUE (Gran Sala), *Parlamento Europeo contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas*, asuntos acumulados C-317/04 y C-318/04, sentencia de 30 de mayo de 2006. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=635858 [consulta: 27 de mayo de 2015].
[968] Magdalena M. MARTÍN MARTÍNEZ (2010), «Terrorismo y derechos humanos en la Unión Europea y en el Consejo de Europa: ¿marco de referencia mundial?», en *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, núm. 1, pág. 421. Disponible en Internet: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2009/2009_10.pdf [consulta: 16 de marzo de 2016].

objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal» (apartado 54). En los considerandos de las Decisiones controvertidas se expone que «*los datos de los PNR se utilizarán únicamente para los fines de prevención y lucha contra el terrorismo y delitos conexos, otros delitos graves, incluida la delincuencia organizada, que tengan un carácter transnacional y la fuga en caso de orden de arresto o detención por estos delitos*» (apartado 55). En consecuencia, el TJUE concluyó que «*la transferencia de los datos de los PNR al CBP constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal*» (apartado 56). En opinión del Tribunal, la transmisión de datos *PNR* con fines comerciales (para vender billetes a cambio de los cuales se prestarían determinados servicios), sí estaba dentro del ámbito del derecho comunitario, sin embargo, el tratamiento de estos datos tal y como se presentaba en la Decisión de la Comisión no perseguía un fin comercial sino una finalidad represiva con el objeto de salvaguardar la seguridad pública[969], y «*no obstante, de ello no se desprende que, debido al hecho de que los datos de los PNR sean recogidos por operadores privados con fines mercantiles y de que sean éstos quienes organizan su transferencia a un Estado tercero, dicha transferencia no esté incluida en el ámbito de aplicación de la citada disposición. En efecto, esta transferencia se inserta en un marco creado por los poderes públicos y cuyo objetivo es proteger la seguridad pública*» (apartado 58). En fin, el Tribunal señala que «*el artículo 95 CE en relación con el artículo 25 de la Directiva no puede constituir la base de la competencia de la Comunidad para celebrar el Acuerdo*» (apartado 67). La sentencia del TJUE deja claro que la Directiva 95/46/CE no es una norma jurídica que pueda servir de parámetro para enjuiciar la validez de diversos actos relacionados con el envío de datos de pasajeros a EE.UU., pues, por tratarse de iniciativas que se enmarcan en la lucha contra el terrorismo, quedan fuera de su ámbito de aplicación[970].

93. Unos meses después la sentencia del TJUE, en octubre de 2006, finalizadas las negociaciones entre la Comisión y los EE.UU., el Consejo de la UE aprobó un Acuerdo provisional ("*interim agreement*") entre la UE y los Estados Unidos, para permitir la continuación de la transferencia de datos *PNR* a los EE.UU. a la espera del acuerdo

[969] TJUE (Gran Sala), *Parlamento Europeo contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas*, apartado 57.

[970] *Vid*. José Luis PIÑAR MAÑAS (2009), «*Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*», en *Fundación Alternativas*, núm. 147, pág. 24. Disponible en Internet: http://www.fundacionalternativas.org/laboratorio/documentos/documentos-de-trabajo/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio [consulta: 19 de marzo de 2016].

definitivo[971]. El 23 de julio de 2007 se firmó un nuevo Acuerdo, lo que permitió un *PNR* más amplio, debido a las presiones realizadas por el Departamento de Seguridad Nacional de EE.UU. en la Presidencia del Consejo y la Comisión Europea[972]. Su contenido consiste en mismo documento y una carta de Estados Unidos a la Unión Europea donde se exponen los métodos de conservación, uso y transferencia de datos *PNR* por parte del Departamento de Seguridad del Territorio Nacional (*Department of Homeland Security - DHS*)[973].

94. Sin embargo, la entrada en vigor del Tratado de Lisboa (1 de diciembre de 2009) marcó un punto de inflexión en relación con la protección del derecho a la privacidad y los datos personales, también gracias a una serie de poderes que el Parlamento Europeo adquirió relativos a la conclusión de acuerdos internacionales que resultarían decisivos para un nuevo Acuerdo *PNR*. De hecho, la toma de los nuevos poderes del Parlamento Europeo[974] no se hizo esperar: el 5 de mayo de 2010, el Parlamento Europeo adoptó una Resolución en la que pedía una renegociación del Acuerdo *PNR* de 2007[975]. El Parlamento pidió que cualquier nuevo instrumento legislativo sobre *PNR* fuese precedida de una evaluación de impacto sobre la privacidad y un test de proporcionalidad con el fin de demostrar la insuficiencia de los instrumentos jurídicos existentes[976]. El 2 de diciembre de 2010, el Consejo autorizó a la

[971] Joan Lluís PÉREZ FRANCESCH, Tomás GIL MÁRQUEZ, Alejandro GACITÚA ESPÓSITO (2011: 11); DECISIÓN 2006/729/PESC/JAI DEL CONSEJO, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, *Diario Oficial de la Unión Europea*, L 298, 27.10.2006, págs. 27–31.

[972] DECISIÓN 2007/551/PESC/JAI DEL CONSEJO, de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo *PNR* 2007). Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo *PNR* 2007), *Diario Oficial de la Unión Europea*, L 204, 4.8.2007, págs. 16–25. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2007.204.01.0016.01.SPA [consulta: 25 de marzo de 2016].

[973] Joan Lluís PÉREZ FRANCESCH, Tomás GIL MÁRQUEZ, Alejandro GACITÚA ESPÓSITO (2011: 12).

[974] En particular, la concesión de poder de veto en manos del Parlamento Europeo (según el artículo 218 del TFUE) respecto a los acuerdos internacionales de conformidad en ámbitos por el procedimiento legislativo ordinario.

[975] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 5 de mayo de 2010, sobre el inicio de las negociaciones para los acuerdos relativos al registro de nombres de los pasajeros (PNR) con los Estados Unidos, Australia y Canadá, *Diario Oficial de la Unión Europea*, C 81E, 15.3.2011, págs. 70–74. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010IP0144 [consulta: 28 de marzo de 2016].

[976] También era necesaria una limitación con respecto a la cantidad de datos recopilados. En su Resolución, el Parlamento también prohibió el estudio de los perfiles elaborados con la extracción de datos. Por último, había que garantizar el control jurídico y democrático.

Comisión a negociar un nuevo Acuerdo con EE.UU. y las conversaciones empezaron inmediatamente[977].

95. Tras la aprobación por parte del Parlamento[978], el Consejo adoptó la Decisión de 26 de abril de 2012, relativa a la celebración del Acuerdo entre los EE.UU. de América y la UE sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los EE.UU., que sustituyó al anterior Acuerdo *PNR* entre la Unión Europea y los EE.UU. que se había aplicado de forma provisional desde 2007[979].

96. En comparación con los acuerdos previos, el nuevo Acuerdo *PNR* de 2012[980] ("*U.S.-EU PNR Agreement*") (en adelante, Acuerdo *PNR* UE-EE.UU.) prevé algunas garantías para proteger los datos que fueron consideradas insuficientes por el Grupo de Trabajo[981] y el SEPD[982]. El Acuerdo proporciona una base jurídica para la "utilización y la transferencia de

[977] Tras la reanudación de las negociaciones, la Comisión reiteró, en noviembre de 2011, una nueva propuesta de acuerdo con el Parlamento. *Vid*. PROPUESTA DE DECISIÓN DEL CONSEJO relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, COM(2011) 807 final, Bruselas, 23.11.2011.

[978] Un peso significativo en esta aprobación, contrariamente a las elecciones hechas anteriormente por el Parlamento, fue con certeza el de las presiones políticas ejercidas por los EE.UU. El gobierno americano de hecho había amenazado con suspender los viajes sin visado a los EE.UU.

[979] DECISIÓN DEL CONSEJO de 26 de abril de 2012 relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (2012/472/UE), *Diario Oficial de la Unión Europea*, L 215/4, 11.8.2012. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:JOL_2012_215_R_0004_01&from=IT [consulta: 02 de abril de 2016].

[980] ACUERDO entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, *Diario Oficial de la Unión Europea*, L 215/5, 11.8.2012. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22012A0811(01) [consulta: 02 de abril de 2016]. El Acuerdo permanecerá en vigor durante un período de siete años (hasta 2019) a partir de su entrada en vigor (2012).

[981] ARTICLE 29 DATA PROTECTION WORKING PARTY (2012a), Letter from the Article 29 Working Party addressed to Members of the LIBE Committee of the European Parliament, Brussels, 6 January 2012. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf [consulta: 03 de abril de 2016]. Las críticas levantadas sobre este Acuerdo se identifican en la ausencia de una mayor protección para los datos sensibles, la excesiva duración de la retención de datos, el hecho de no elaborar mecanismos apropiados de acceso y recurso, ante la falta de claridad sobre la frecuencia de las transferencias, o en la evaluación de la adecuación del nivel de protección de datos en EE.UU.

[982] DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, *Diario Oficial de la Unión Europea*, C 181, 22.6.2011, págs. 24–30. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52011XX0622%2802%29 [consulta: 09 de abril de 2016]. Las críticas levantadas por el Supervisor evidencian la incompatibilidad de tales instrumentos con relación a la protección de los datos personales y la vida privada de los ciudadanos.

los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los EE.UU."[983].

97. El Acuerdo *PNR* de 2012 prevé que el Departamento de Seguridad del Territorio Nacional de los EE.UU. conserve los datos *PNR* en una base de datos durante cinco años. Después de los primeros seis meses, la información que hace posible identificar directamente a un pasajero está enmascarada y despersonalizada. Al cabo de cinco años, los datos se trasladan a una «*base de datos inactiva durante un período de hasta 10 años*», pero con «*controles adicionales, incluido un número más restringido de miembros del personal autorizados, así como la exigencia de una aprobación de supervisión de nivel superior previa al acceso*»[984]. Además, los datos sensibles sólo se permiten en casos excepcionales y se podrá acceder a dichos datos utilizando «*exclusivamente procedimientos restrictivos*» y, en cada caso, con la aprobación de un directivo del Departamento de Seguridad de EE.UU.[985]. A continuación, serán eliminados de forma permanente por el mismo

[983] La UE ha preferido regular las relaciones con los EE.UU., su principal socio estratégico, a través de acuerdos verticales para evitar las dificultades asociadas a una evaluación global de la adecuación, dadas las peculiaridades de la legislación estadounidense, que adopta un enfoque sectorial. Sobre este aspecto, el RGPD contiene una cláusula de salvaguardia de «*los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales*», pero no limita expresamente la exclusión de su aplicabilidad a los acuerdos previos a su adopción. Nos referimos al considerando 102 del RGPD: «*El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados*». A este respecto, el estado en que las cosas estaban antes no se ha modificado, ya que no se ha previsto ninguna disposición que requiera la revisión de los acuerdos anteriores a fin de adecuarlos al nuevo marco general de protección de datos personales. Aquí, anticipando el artículo 50 del RGPD, se expresa la firme voluntad de la UE de tratar con terceros Países con el fin de promover una protección más eficaz de los derechos individuales con respecto a los datos personales, dando testimonio de la voluntad de cooperar con las autoridades extranjeras, pero la realización efectiva y el éxito de las formas de cooperación internacional dependerán en gran medida de la voluntad del diálogo expresado por los socios de la UE. Sin embargo, el régimen de extraterritorialidad de la aplicación del RGPD puede contribuir, en parte, a aumentar el peso de la UE en las negociaciones internacionales. Artículo 50 (Cooperación internacional en el ámbito de la protección de datos personales) del RGPD: «*En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para: a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales; b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales; c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales; d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países*».

[984] Artículo 8 (Conservación de los datos), apartados de 1-3, del Acuerdo *PNR* UE-EE.UU.

[985] Es decir, «*información y datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la sexualidad*

Departamento en los «*30 días siguientes a la última recepción del PNR que los contenga*», a menos que se utilicen «*para realizar una acción específica de investigación, enjuiciamiento o ejecución*»[986]. Finalmente, cada persona, independientemente de su nacionalidad, país de origen o lugar de residencia, cuyos datos personales e información personal hayan sido tratados y utilizados de forma no conforme con el presente Acuerdo, podrá presentar un recurso efectivo por vía administrativa y judicial con arreglo a la legislación de los EE.UU.

98. A pesar de que el objetivo de la utilización de datos *PNR* es combatir el terrorismo y la delincuencia transnacional grave[987], se puede comprobar que el Acuerdo de 2012 no satisfacía muchas de las demandas que el Parlamento Europeo había incluido en su Resolución de 2010. Más específicamente, el período de retención de datos no se reduce sino sigue siendo extraordinariamente largo. Los datos conservados serán convertidos sólo parcialmente en datos anónimos. Tampoco el Acuerdo, prohíbe explícitamente la "minería de datos" ("*data mining*") y el "perfilado" ("*profiling*") de personas. Además, los derechos de los ciudadanos no parecen estar efectivamente salvaguardados[988]: toda persona, de conformidad con la Ley de Libertad de la Información ("*Freedom of Information Act*"), tiene derecho a solicitar su *PNR* al Departamento de Seguridad de EE.UU, pero el Acuerdo no especifica las obligaciones de las autoridades estadunidenses, que pueden rechazar la solicitud; no hay prueba de la necesidad y proporcionalidad de las medidas adoptadas en el Acuerdo a los fines de lucha contra el terrorismo; por último, no parece ofrecer garantías suficientes en lo que respecta a las transferencias a terceros Países.

99. Por lo tanto, el Acuerdo *PNR* EU-EE.UU. de 2012 parece, pues, una victoria de los intereses políticos a expensas del derecho a la protección de datos personales de los ciudadanos europeos.

de la persona». Estos datos pueden obtenerse, por ejemplo, mediante elecciones religiosas de alimentos. Artículo 6 (Datos sensibles), apartado 3, del Acuerdo *PNR* UE-EE.UU.

[986] Artículo 6 (Datos sensibles), apartado 4, del Acuerdo *PNR* UE-EE.UU.

[987] *Amplius* artículo 4 (Utilización de los PNR) del Acuerdo *PNR* UE-EE.UU.

[988] «Is the new EU-US PNR Agreement acceptable?», en *European Digital Rights (EDRi)*, 2012, págs. 2. Disponible en Internet: https://edri.org/files/2012EDRi_US_PNRcomments.pdf [consulta: 13 de abril de 2016].

2.6.2. Equilibrio entre seguridad y protección de los derechos fundamentales: análisis de la Directiva 2016/681 sobre el uso del registro de nombre de pasajero (PNR)

100. El 6 de noviembre de 2007, la Comisión adoptó la Propuesta de Decisión Marco del Consejo sobre utilización de datos del registro de nombres de los pasajeros con fines policiales en la UE[989]. No obstante, al entrar en vigor el Tratado de Lisboa, «*la Propuesta de la Comisión*», que en aquella fecha «*todavía no había sido aprobada por el Consejo, quedó obsoleta*»[990]. Tras la presentación de una Propuesta de Directiva por parte de la Comisión Europea en el 2011, el procedimiento legislativo quedó bloqueado cuando la

[989] La propuesta de Decisión Marco contaba con 20 artículos estructurados en cinco capítulos, y tenía como objetivo regular «*la puesta a disposición de las autoridades competentes de los Estados miembros de los datos PNR de los pasajeros de los vuelos internacionales por parte de las compañías aéreas a efectos de la prevención y lucha contra los delitos terroristas y la delincuencia organizada, así como la recogida y conservación de tales datos por parte de dichas autoridades y su intercambio entre ellas*» (artículo 1 - Objetivos). *Vid*. PROPUESTA DE DECISIÓN MARCO DEL CONSEJO sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record - PNR) con fines represivos, 2007/0237 (CNS), Bruselas, 6.11.2007, COM(2007) 654 final. Disponible en Internet: http://www.fomento.gob.es/AZ.BBMF.Web/documentacion/pdf/com2007_0654.pdf [consulta: 17 de abril de 2016].

[990] PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, COM/2011/0032 final - COD 2011/0023, Bruselas, 2.2.2011. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52011PC0032 [consulta: 17 de abril de 2016]. En febrero de 2011, la Comisión presentó una propuesta de Directiva sobre los datos de los pasajeros para combatir las formas graves de delincuencia y el terrorismo (es decir, *PNR* de la UE). *Vid*. COMISIÓN EUROPEA - Press Release (2011), Propuesta de la UE sobre los datos de los pasajeros para combatir las formas graves de delincuencia y el terrorismo, Bruselas, 2 de febrero de 2011. Disponible en Internet: http://europa.eu/rapid/press-release_IP-11-120_es.htm [consulta: 17 de abril de 2016]. El 5 de abril de 2011, el Grupo de Trabajo emitió una opinión negativa al respecto. El Grupo de Trabajo evaluó críticamente los aspectos de necesidad y proporcionalidad que no justificaban la limitación de los derechos y libertades fundamentales. Según el Grupo de Trabajo, no hay pruebas de que el tratamiento de los datos de los *PNR* en todos los Estados miembros evite las brechas de seguridad debidas a la supresión de las fronteras interiores. Cabe señalar que el tratamiento de datos *PNR* como herramientas de inteligencia implica también un aumento del nivel de los requisitos de seguridad exigidos en el ámbito de la protección de datos. Sin embargo, debe evaluarse si los instrumentos de cooperación judicial no son los instrumentos más adecuados para el mismo fin. Además, la recogida de todos los datos de todas las personas sobre los vuelos es una medida desproporcionada que está en conflicto con el artículo 8 de la CDFUE. ARTICLE 29 DATA PROTECTION WORKING PARTY (2011a), Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 00664/11/EN, WP 181, adopted on 5 April 2011, págs. 9. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp181_en.pdf [consulta: 21 de abril de 2016]. Otra opinión crítica a la Propuesta *PNR* es la de la Agencia Europea de Derechos Fundamentales. *Vid*. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2011b), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)*, FRA Opinion - 1/2011, Vienna, 14 June 2011, págs. 23. En junio de 2011, también el SEPD emitió su dictamen sobre la Propuesta de Directiva de la Comisión. El SEPD tomó nota de los progresos realizados para limitar el alcance de la propuesta y las condiciones para el tratamiento de los datos *PNR*. Sin embargo, su opinión era contraria, ya que no se cumplían los requisitos esenciales de necesidad y proporcionalidad. Considera que los datos *PNR* sólo deben tomarse para casos específicos. Otras deficiencias identificadas por el SEPD es su excesivo ámbito de aplicación. La naturaleza de las amenazas que permiten el intercambio de datos debe definirse con mayor claridad. Los datos deben almacenarse en forma identificable durante un período no superior a 30 días y luego enmascararlos. Por último, dentro de los datos *PNR*, los elementos tratados deben reducirse. Vid. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011).

Comisión de Libertades Civiles, Justicia y Asuntos de Interior (en adelante, Comisión LIBE) del Parlamento Europeo rechazó la Propuesta de *PNR* de la UE en abril de 2013, cuestionando su necesidad, proporcionalidad y su respeto a los derechos fundamentales[991]. Sin embargo, el Pleno del Parlamento en junio de 2013 y el Consejo en 2014 decidieron seguir adelante con ello[992].

101. Por lo tanto, después de años de negociaciones, se alcanza un Acuerdo entre el Parlamento y Consejo[993], sobre la Directiva europea relativa al registro de nombres de pasajeros, para la prevención, detección, investigación y enjuiciamiento de los delitos terroristas y los delitos graves, aprobado por la Comisión LIBE[994] del Parlamento Europeo el 10 de diciembre de 2015.

102. El principal motivo que ha alentado este Acuerdo que permaneció durante años bloqueado, ha sido la creciente preocupación por la amenaza terrorista que vive Europa con los sucesivos s atentados terroristas, y las nuevas preocupaciones relativas a posibles amenazas a la seguridad interior de la Unión que plantean los "combatientes extranjeros". Esta situación ha empujado a los Estados de la UE y a sus instituciones a reevaluar sus

[991] El resultado de la votación fue: 30 votos en contra de la Propuesta y 25 a favor. La mayoría de los miembros de la Comisión LIBE en su oposición a la Propuesta reanudaron las motivaciones ya expresadas por el Grupo de Trabajo y el SEPD. Concretamente, cuestionaron la proporcionalidad de la recopilación, utilización y almacenamiento de los datos por parte de las compañías aéreas, sobre todo por el hecho de que esto sucede indiferentemente que un individuo sea o no un sospechoso. Se hace hincapié en que no está de acuerdo con los derechos fundamentales, en particular con la protección de datos. Por otra parte, la razón de la minoría que había votado a favor de la Propuesta dio lugar al potencial valor añadido que esta directiva podría haber llevado a los efectos del antiterrorismo europeo. Por otra parte, añadiendo que la consecución de un modelo europeo único habría sido una opción mejor que la de entonces, de diferentes decisiones individuales para cada Estado miembro. PARLAMENTO EUROPEO - Notas de prensa (2013), Civil Liberties Committee rejects EU Passenger Name Record proposal, 24-04-2013. Disponible en Internet: http://www.europarl.europa.eu/news/es/press-room/20130422IPR07523/civil-liberties-committee-rejects-eu-passenger-name-record-proposal [consulta: 27 de abril de 2016].

[992] EUROPEAN PARLIAMENT (2016), EU Passenger Name Record (PNR) directive: an overview, 01-06-2016, pág. 5. La propuesta de Directiva *PNR* obliga a las compañías aéreas a transmitir a los Países de la UE los datos de sus pasajeros (itinerario, modo de pago, equipaje, frecuencia con que vuela, *etc*.) con el fin de ayudar a las autoridades para luchar contra el terrorismo y otros delitos graves. Esto permitiría una recopilación más sistemática, uso y conservación de los datos *PNR* de los pasajeros de líneas aéreas, y por lo tanto tiene un impacto directo sobre los derechos de privacidad y protección de datos, poniendo en peligro el principio de proporcionalidad y las garantías que deberían poner en marcha para la protección de los datos personales.

[993] En este contexto, el Consejo Europeo instó al Parlamento Europeo a trabajar rápidamente para llegar a un acuerdo sobre una directiva sobre los *PNR*. También subrayó la importancia de trabajar en un enfoque coherente con los adoptados por terceros Países y, por lo tanto, recomendó una estrecha cooperación. CONSEJO EUROPEO (2014), Reunión extraordinaria del Consejo Europeo, Bruselas, 30.8.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/european-council/2014/08/30/ [consulta: 30 de abril de 2016].

[994] El 19 de marzo de 2015, el Grupo de Trabajo envió una carta a la Comisión LIBE, señalando que el *PNR* no respeta los principios de necesidad y proporcionalidad, como exige la CDFUE (artículos 7 y 8). ARTICLE 29 DATA PROTECTION WORKING PARTY (2015a), Letter on EU PNR, Brussels, 19th March 2015. Disponible en Internet: http://www.statewatch.org/news/2015/mar/eu-pnr-letter-art-29-wp-to-chair-libe.pdf [consulta: 30 de abril de 2016].

políticas de seguridad, y proponer nuevas iniciativas para reforzar la lucha antiterrorista, en concreto en el establecimiento de controles sistemáticos de fronteras, control de armas y registro de pasajeros. En particular, los Jefes de Estado reunidos en Bruselas el 12 de febrero de 2015 pusieron el asunto sobre la Directiva *PNR* como la primera prioridad de las necesidades inmediatas y urgentes con el fin de garantizar la seguridad de los ciudadanos[995]. En diciembre de 2015, el Parlamento y el Consejo alcanzaron una solución de compromiso sobre esta delicada cuestión[996].

103. Finalmente, el 21 de abril de 2016, el Consejo hizo suya la posición adoptada por el Parlamento en primera lectura[997], concluyendo así el procedimiento legislativo sobre esta propuesta. El 27 de abril de 2016, la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[998] (en adelante, Directiva *PNR*) fue aprobada con 461 votos a favor, 179 en contra y 9 abstenciones, y firmada por el presidente del Parlamento Europeo, y por el

[995] CONSEJO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA (2015), Reunión informal de los jefes de Estado o de Gobierno, Bruselas, 12 de febrero de 2015.

[996] Críticas muy fuertes llegaron a la propuesta de Directiva por el SEPD. El Supervisor denuncia que la propuesta no cumple las normas establecidas en los artículos 7, 8 y 52 de la CDFUE, el artículo 16 del TFUE y el artículo 8 del CEDH. Vid. RESUMEN EJECUTIVO DEL SEGUNDO DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, *Diario Oficial de la Unión Europea*, C 392, 25.11.2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2015_392_R_0009&from=ES [consulta: 03 de mayo de 2016].

[997] El 14 de abril de 2016, el Parlamento Europeo aprobó la Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

[998] DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, *Diario Oficial de la Unión Europea*, L 119, 4.5.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0681&from=ES [consulta: 05 de mayo de 2016].

Ministro de Defensa de los Países Bajos en nombre del Consejo. Los Estados miembros estaban obligados a transponer[999] la Directiva *PNR* a más tardar el 25 de mayo de 2018[1000].

104. El objetivo de la nueva Directiva *PNR* es proporcionar un medio adicional de investigación para las fuerzas de inteligencia y policía en la acción de prevención, detección e investigación de delitos de terrorismo y delincuencia grave[1001].

105. El impulso a esta nueva normativa ha sido posible gracias a la consecución de un compromiso difícil, ya que, junto con la Directiva *PNR*, el Parlamento dio vía libre a dos medidas distintas, un Reglamento y una Directiva sobre protección de datos individuales de los ciudadanos, que permitían encontrar un equilibrio entre la necesidad de reforzar la seguridad y proteger la privacidad en la era digital[1002]. Esto explica que la Directiva *PNR* se haya adoptado en el mismo contexto de la promulgación del "paquete" de protección de los datos personales europeo, lo que supone un mensaje favorable a comenzar el camino de regulación compartida del ciberespacio y de todos los fenómenos relacionados. En todo caso, la Directiva *PNR* ha sido, y sigue siendo, un acuerdo controvertido, cuyos contornos hay todavía que examinar y definir con más precisión.

106. La Directiva *PNR* establece "normas armonizadas para la recogida y el tratamiento de datos *PNR*[1003] destinados a la prevención, detección, investigación y enjuiciamiento de

[999] En la actualidad, Italia ha traspuesto las nuevas normas relativas a los datos del registro de nombres de los pasajeros, en vigor desde el 09 de junio de 2018, en su legislación nacional. *Vid*. Decreto Legislativo 21 maggio 2018, n. 53. Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004. (18G00081) (*GU Serie Generale* n.120 del 25-05-2018). España, y otros 13 países (Austria, Bulgaria, Chequia, Chipre, Eslovenia, Estonia, Finlandia, Francia, Grecia, Luxemburgo, Países Bajos, Portugal y Rumanía), no han adoptado la legislación nacional que transpone plenamente la Directiva *PNR*. En este sentido, la Comisión ha instado, enviando cartas de emplazamiento, a los 14 Estados miembros a transponer las nuevas normas relativas a los datos del registro de nombres de los pasajeros (PNR). COMISIÓN EUROPEA - Hoja informativa (2018), Paquete de procedimientos de infracción correspondiente al mes de julio: principales decisiones, Bruselas, 19 de julio de 2018, MEMO/18/4486.

[1000] La Comisión Europea llevará a cabo una revisión de la Directiva europea sobre *PNR* dos años después de su transposición a la legislación nacional.

[1001] Las bases jurídicas para la adopción de la Directiva (UE) 2016/681 (el TFUE y, en particular, su artículo 82, apartado 1, letra d), y su artículo 87, apartado 2, letra a), son un claro ejemplo de la voluntad del legislador europeo de armonizar las disposiciones de los Estados miembros sobre la conservación de determinados datos generados o tratados por las compañías aéreas para reforzar la cooperación entre la policía y la autoridad judicial y garantizar que los datos estarían disponibles para la investigación, detección y enjuiciamiento de delitos terroristas y delitos graves.

[1002] Costanza DI FRANCESCO MAESA (2016).

[1003] A efectos de la presente Directiva, artículo 3 (Definiciones), se entenderá por «(…) *«registro de nombres de los pasajeros» o «PNR»: una relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías*

delitos terroristas y delitos graves"[1004]. De conformidad con la Directiva, las compañías aéreas están obligadas a facilitar a los países de la UE los datos de sus pasajeros para ayudar a las autoridades a combatir el terrorismo y la delincuencia grave teniendo plenamente en cuenta «*el derecho a la protección de los datos personales y el derecho a la no discriminación*»[1005]. La Directiva se aplica a los vuelos exteriores de la UE, pero los Estados miembros tienen la posibilidad también de aumentar esa obligación a las compañías aéreas que efectúan vuelos interiores de la UE[1006], siempre que lo notifiquen por escrito a la Comisión y se publique en el Diario Oficial de la UE[1007]. Por tanto, de acuerdo con su contenido, todas las compañías aéreas estarán obligadas a conservar e intercambiar los datos relativos a todos los vuelos hacia y desde Europa. Esta medida es considerada imprescidible por los Estados europeos para detectar los movimientos de los yihadistas en el Espacio Schengen[1008].

107. La Directiva establece que la transferencia de datos *PNR* sólo debe permitirse «*caso por caso*»[1009] ("*case-by-case basis*") y respetando plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la Decisión Marco 2008/977/JAI[1010]. La Directiva

aéreas que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades».

[1004] PARLAMENTO EUROPEO - Notas de prensa (2016a), El Parlamento aprueba la directiva sobre registro de datos de pasajeros (PNR), 14-04-2016. Disponible en Internet: http://www.europarl.europa.eu/news/es/news-room/20160407IPR21775/el-parlamento-aprueba-la-directiva-sobre-registro-de-datos-de-pasajeros-(pnr) [consulta: 01 de junio de 2016]. Como señaló el eurodiputado responsable de la tramitación parlamentaria del texto, Timothy Kirkhope (ECR, Reino Unido), «*se trata de una herramienta importante para luchar contra los terroristas y traficantes. Mediante la recogida, intercambio y análisis de los datos PNR, nuestros servicios de inteligencia pueden detectar patrones de comportamiento sospechoso que merecen seguimiento. La directiva PNR no es una fórmula mágica, pero los países que ya tienen sistemas nacionales de registro de datos han demostrado que es un instrumento muy efectivo*». El mismo agregó «*comprendo las reservas sobre la obtención y almacenamiento de datos personales, pero creo que la propuesta incluye salvaguardas, y también demuestra que es proporcionada en relación a los riesgos que enfrentamos. Los gobiernos de la UE deben ahora ponerse a la tarea de aplicar el acuerdo*».

[1005] Considerando 20 de la Directiva *PNR*.

[1006] Considerando 10 de la Directiva *PNR*.

[1007] Artículo 2 (Aplicación de la presente Directiva a los vuelos interiores de la UE) de la Directiva *PNR*. Una vez que el Estado miembro ha acordado la obligación de recogida de datos *PNR* a todos o a determinados vuelos internos, se aplicarán las normas generales de la presente Directiva para los datos *PNR* de quienes realicen esos vuelos. El Estado miembro puede en cualquier momento comunicar a la Comisión, también por escrito y también con publicación en el DOUE, su decisión de revocar la aplicación de la Directiva a los vuelos interiores.

[1008] Aunque se benefician de una excepción, Reino Unido e Irlanda han decidido participar en esta Directiva. Dinamarca es el único de los 28 Estados miembros que no estará en el *PNR* europeo. Los gobiernos de la UE también pueden decidir proceder a la recogida y tratamiento de los datos *PNR* de los diferentes agentes económicos de las compañías aéreas, como las agencias de viaje y operadores turísticos, que ofrecen servicios de reserva de vuelo.

[1009] Considerando 31 de la Directiva *PNR*.

[1010] La Directiva sólo se refiere a los medios generales de reparación previstos en el Derecho de la Unión y nacional y en la aplicación de los artículos 17, 18, 19 y 20 de la Decisión Marco 2008/977/JAI, sin indicar

tiene por objeto: a) «*la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE*»; b) «*el tratamiento de los datos*» mismos, «*incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros*». Los datos *PNR* obtenidos «*podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves*»[1011]. Se autoriza, por tanto, la utilización de estos datos *PNR*, que suponen una injerencia significativa en derechos fundamentales de los ciudadanos, para la persecución de «*delitos graves* (…) *que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al derecho nacional de un Estado miembro*»[1012]. Debe considerarse que la conservación de datos con el fin de consentir a las autoridades nacionales competentes el acceso a dichos datos, tal como establece la Directiva *PNR*, responde a un objetivo de interés general[1013]. El hecho de que la lucha contra el terrorismo internacional para mantener la paz y la seguridad internacionales, como lo mismo sucede con la lucha contra la delincuencia grave para garantizar la seguridad pública, constituyen un objetivo de interés general que se desprende de la jurisprudencia del TJUE[1014].

108. El *PNR* europeo se basa en un sistema descentralizado e interconectado. Los Estados miembros tienen que establecer su propia "unidad única de información sobre los pasajeros" (en adelante, UIP)[1015] para recoger datos *PNR* de las compañías aéreas[1016]. Estos datos se

ningún medio específico de reparación. Artículo 13 (Protección de los datos de carácter personal), apartado 1, de la Directiva *PNR*.

[1011] Artículo 1 (Objeto y ámbito de aplicación) de la Directiva *PNR*.

[1012] Por lo que respecta a las definiciones de "delitos graves", cabe destacar la lista de los delitos a la que se refiere el artículo 3, punto 9, son los incluidos en el Anexo II de la Directiva *PNR*.

[1013] CONSEJO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA (2017).

[1014] Se remite *supra* a las sentencias del TJUE.

[1015] Considerando 13 de la Directiva *PNR*. La UIP será responsable de la recogida, almacenamiento y procesamiento de datos *PNR* y de transferirlos a las autoridades competentes e intercambiarlos con las Unidad de Información sobre los Pasajeros de otros Estados miembros y con Europol. *Vid*. artículo 4 (Unidad de Información sobre los Pasajeros) de la Directiva *PNR*. Para garantizar la protección de datos, en los datos *PNR* que las compañías aéreas están obligadas a recoger y proporcionar a las autoridades competentes designadas como Unidad de Información sobre los Pasajeros en cada Estado miembro, no se incluyen los "datos sensibles", que son los que revelen «*el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona*. *En el caso de que la UIP reciba datos PNR que revelen tal información, los suprimirá inmediatamente*». Artículo 13 (Protección de los datos de carácter personal), apartado 4, de la Directiva *PNR*. Sobre este tema, véanse DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011: núms. 6, 46, 47 y 50).

[1016] La UIP recibe los datos *PNR* de las compañías aéreas por el método de transmisión, «*por el cual las compañías aéreas envían los datos PNR incluidos en el anexo I a la base de datos de la autoridad requirente*». artículo 3, núm. 7. Las aerolíneas estarán obligadas a transferir electrónicamente toda la información a estas unidades en dos ocasiones: 1) «*24 a 48 horas antes de la salida programada del vuelo*»; 2) «*inmediatamente después del cierre*», una vez que todos los pasajeros estén embarcados y no sea posible que entre nadie más. Artículo 8 (Obligaciones de las compañías aéreas en relación con la transmisión de datos), apartado 3. Las compañías que no cumplan serán sancionadas con multas que debe fijar cada Estado miembro. Las compañías

conservarán durante «*un período de cinco años*»[1017], si bien después de seis meses de la transferencia todos los datos *PNR* deben ser «*despersonalizados mediante enmascaramiento*» de algunos «*elementos que podrían servir para identificar directamente al pasajero al que se refieren los datos PNR*», tales como nombre y apellido, dirección y datos de contacto[1018]. El periodo de conservación de los datos ha sido una de las cuestiones más polémicas durante la larga tramitación de esta Directiva. Los gobiernos reclamaban un plazo amplio mientras que el Parlamento Europeo quería restringirlo al máximo para limitar el impacto en la privacidad.

aéreas mandarán los datos con el método llamado "*push*", en el sentido de que los Estados miembros no tienen «*acceso directo a los sistemas informáticos de las compañías*», permitiendo así a las compañías aéreas mantener el control sobre lo que se proporcionan datos, en lugar del método "*pull*", con el que las autoridades competentes del Estado miembro que soliciten los datos *PNR* pueden acceder al sistema de reservas de la compañía aérea y extraer ("*pull*") una copia de los datos *PNR* requeridos. Esto es otro indicador de la tentativa hecha por el legislador de la UE para proporcionar garantías procesales para la protección de datos. Esto supone, por tanto, que son las compañías aéreas las que suministran los datos a la UIP, y no la UIP la que puede acceder a las bases de datos de las compañías aéreas y recabar los datos que consideren necesarios. Como dicho, la Directiva *PNR* incorpora como Anexo I los datos *PNR* que están obligadas a recopilar las compañías aéreas y que incluye un total de 19 datos PNR: «*1. Localizador de registro PNR. 2. Fecha de reserva/emisión del billete. 3. Fecha(s) o fechas de viaje prevista(s). 4. Nombre(s) y apellido(s). 5. Dirección y datos de contacto (número de teléfono, dirección de correo electrónico). 6. Todos los datos de pago, incluida la dirección de facturación. 7. Itinerario completo del viaje para el PNR específico. 8. Información sobre viajeros asiduos. 9. Agencia de viajes/operador de viajes. 10. Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva. 11. Información PNR escindida/dividida. 12. Observaciones generales (incluida la información disponible sobre menores de 18 años no acompañados como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculos con el menor, agente en el lugar de salida y de llegada). 13. Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote). 14. Datos del asiento, incluido el número. 15. Información sobre códigos compartidos. 16. Toda la información relativa al equipaje. 17. Número de viajeros y otros nombres de viajeros que figuran en el PNR. 18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) (incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada). 19. Todo el historial de cambios de los datos PNR indicados en los números 1 a 18*».

[1017] Artículo 13 (Protección de los datos de carácter personal), apartado 6, de la Directiva *PNR*.

[1018] Artículo 12 (Período de conservación de los datos y despersonalización) de la Directiva *PNR*: «*1. Los Estados miembros se asegurarán de que los datos PNR proporcionados por las compañías aéreas a la UIP se conservan en una base de datos de la Unidad durante un plazo de cinco años a partir de su transmisión a la UIP del Estado miembro en cuyo territorio tenga su punto de aterrizaje u origen el vuelo. 2. Al finalizar un plazo de seis meses desde la transmisión de datos PNR mencionada en el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento de los siguientes elementos que podrían servir para identificar directamente al pasajero al que se refieren los datos PNR: a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas; b) dirección y datos de contacto; c) rodos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona; d) información sobre viajeros asiduos; e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y f) toda la API recopilada*».

109. Resulta necesario aclarar que la despersonalización de los datos *PNR*, una vez transcurridos los seis primeros meses, no es, sin embargo, definitiva, ya que estos datos pueden ser nuevamente personalizados. La Directiva condiciona ese procedimiento de «*repersonalización*»[1019] de los datos *PNR* al cumplimiento de dos requisitos, que deben darse simultáneamente, cuando: «*se crea razonablemente que es necesario*»[1020] a los efectos de «*responder en cada caso particular a las peticiones debidamente razonadas*» y con suficiente base de las autoridades competentes «*en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves*»[1021]; y, que la divulgación de los datos repersonalizados haya sido aprobada por: «*i) una autoridad judicial, u ii) otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión a posteriori del responsable de la protección de datos de la UIP*» (artículo 12, apartado 3, letra b).

110. La ausencia de reglas claras y precisas sobre el período de conservación de datos es evidente. En la Directiva se exige que los datos se conserven durante un período de seis meses, tras el cual deberían hacerse accesibles quitando los elementos reconocidos por el artículo 12, apartado 2, que puedan dar lugar a la identificación de individuos; a este respecto, no se hace ninguna distinción en función de su posible utilidad o los fines del objetivo perseguido o de las personas afectadas. Además, se indica que los datos *PNR* deben conservarse durante un período de cinco años, sin posibilidad de variar el período de retención sobre la base de criterios objetivos para garantizar que el período se limite a lo estrictamente necesario[1022]. Los datos nuevamente personalizados, dejan muchas cuestiones abiertas, en tanto el contenido de la Directiva tiene que ser traspuesto por los ordenamientos internos de los distintos Estados miembros, lo que puede plantear problemas de los supuestos en los que cada Estado entenderá «*razonablemente que es necesario*»[1023]; en segundo lugar, no estaría de más que la Directiva obligase a los Estados miembros a que la autorización

[1019] María Ángeles CATALINA BENAVENTE (2016), «La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave», en *Diario La Ley*, núm. 8801, 12 de julio.
[1020] Artículo 12, apartado 3, letra a), de la Directiva *PNR*.
[1021] A los efectos establecidos en el artículo 6, apartado 2, letra b), de la Directiva *PNR*.
[1022] La ONG *European Digital Rights* asegura que un periodo de retención de datos de cinco años es demasiado largo, que la directiva no impide el tratamiento discriminatorio de pasajeros con la elaboración de perfiles de riesgo, y que será una herramienta ineficaz contra el terrorismo. Según la organización «*La directiva PNR es una vergüenza*». Vid. Juan SANHERMELANDO (2016), «La Eurocámara aprueba retener los datos de los pasajeros aéreos para la lucha antiterrorista», en *El Español*, 14.04.2016.
[1023] Artículo 12, apartado 3, letra a), de la Directiva *PNR*.

para suministrar datos que ya han sido despersonalizados recayese siempre en una autoridad judicial.

111. También, parece bastante amplio el poder que se otorga a la UIP ya que, por un lado, esta unidad recibe de las compañías aéreas los datos *PNR* de todos los pasajeros y, por otro, tiene extensas competencias para el tratamiento de dichos datos[1024].

112. La recogida, conservación, procesamiento y transmisión de los datos *PNR* por las UIP tienen como finalidad, como ya se ha indicado, la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de determinados delitos graves. En ese sentido, el considerando 7 de la Directiva *PNR* establece que la evaluación de los datos *PNR* permite la «*identificación de personas no sospechosas de estar implicadas en delitos de terrorismo o en delitos graves antes de que un análisis de sus datos PNR indique que puedan estar implicadas en los mismos, y deban ser objeto de investigación adicional por parte de las autoridades competentes*». Sin embargo, «*para garantizar que el tratamiento de datos se limite a lo necesario*», el establecimiento y la aplicación de criterios de evaluación deben ser limitados a «*los delitos de terrorismo y a la delincuencia grave*» para las que es pertinente el uso de esos criterios. El cumplimiento de la finalidad de la Directiva lo llevan a cabo las UIPs competentes a través de distintas vías, recogidas en el artículo 6 sobre tratamiento de los datos PNR. Estas competencias incluyen la evaluación del comportamiento de los pasajeros que no son sospechosos de haber cometido infracción alguna y la posibilidad de comparar datos *PNR* con una serie de bases de datos que no son concretadas en la Directiva[1025]. Se puede sacar como conclusión que la Directiva abarca, de manera general y con carácter preventivo[1026] a todas las personas, así como datos personales exhaustivos sobre cada uno de los pasajeros que realizan vuelos exteriores de la UE como interiores, incluso

[1024] La Directiva, sin embargo, se limita a señalar que cada Estado miembro «*establecerá o designará una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves, o una sucursal de esa autoridad, para actuar como su Unidad de Información sobre los Pasajeros («UIP»)*». En artículo 4, apartado 1, de la Directiva *PNR*. El SEPD en su Dictamen de 2011 planteaba unas cuestiones específicas: el carácter y composición de la autoridad designada como UIP; la competencia e integridad del personal de la UIP; las garantías previstas para evitar abusos, de tal manera que el autocontrol debería completarse con un control externo estructurado. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011).

[1025] Artículo 6 (Tratamiento de los datos PNR), apartado 2, de la Directiva *PNR*: «*La UIP tratará los datos PNR solo para realizar: a) una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro, a fin de identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes a que se refiere el artículo 7 y, en su caso, por Europol, de conformidad con el artículo 10, ante la posibilidad de que pudiera estar implicada en un delito de terrorismo o delito grave*».

[1026] Esta evaluación tiene como objetivo que, posteriormente, las autoridades competentes en cada Estado miembro examinen dicha información. Costanza DI FRANCESCO MAESA (2016).

cuando no hay pruebas que puedan sugerir que su conducta tenga un vínculo con delitos graves.

113. Este amplio alcance en el tratamiento de los datos PNR ha sido duramente criticado ya que se ha identificado como una herramienta de «*vigilancia masiva*»[1027] y que «*asusta bastante*»[1028] a pesar de que la Directiva PNR trata de mitigar sus efectos apuntando que se trata de una evaluación que «*se realizará de forma no discriminatoria con arreglo a criterios de evaluación establecidos por su UIP. Estos criterios predeterminados de evaluación deben ser orientados, proporcionados y específicos*» (artículo 6, apartado 4). A modo de garantía adicional frente a este control generalizado de todos los pasajeros[1029], la Directiva prevé que la transmisión de los datos *PNR* de las personas que hayan podido ser identificadas «*solo se llevará a cabo tras un análisis de cada caso y, en caso de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados*» (artículo 6, apartado 6)[1030]. En todo caso las dudas permanecen sobre el respeto al principio de presunción de inocencia, considerando que cada pasajero se presume un sospechoso criminal a menos que su perfil insinúe lo contrario. Y en este mismo sentido, las medidas concretas que los organismos encargados de hacer cumplir la ley pueden tomar sobre la base de los resultados no se especifican adecuadamente.

114. A pesar de las cuestiones críticas mencionadas, cabe destacar que, a diferencia de la Directiva sobre la conservación de datos anulada por el TJUE en la sentencia *Digital Rights Ireland*, la Directiva *PNR* contiene salvaguardias sustantivas y de procedimiento

[1027] Así se expresaba el eurodiputado Jan Philipp Albrecht, del grupo de los Verdes en el Parlamento Europeo: «*A lo que nos oponemos es la recogida masiva de todos los datos de todos los pasajeros durante cinco años, y al análisis automático de todos los datos. Porque eso es simplemente vigilancia masiva, sin ninguna eficacia*». En Gloria RODRÍGUEZ-PINA (2016), «Por qué el PNR de la UE como medida antiterrorista puede ser ilegal», en *Huffington Post*, 14/04/2016. Disponible en Internet: http://www.huffingtonpost.es/2016/04/11/pnr-terrorismo_n_9658260.html [consulta: 09 de junio de 2016]. También, vid. Paul DE HERT, Vagelis PAPAKONSTANTINOU (2015), «Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling», en *New Journal of European Criminal Law*, vol. 6, núm. 2, págs. 160-165.

[1028] En María Ángeles CATALINA BENAVENTE (2016).

[1029] María Ángeles CATALINA BENAVENTE (2016).

[1030] Los fines propios de la Directiva se cumplen, a través del control de los pasajeros tras la recepción de: «*b) responder en cada caso particular, a las peticiones debidamente razonadas y con suficiente base de las autoridades competentes de que se suministren y traten datos PNR en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y facilitar a las autoridades competentes o, en su caso, a Europol, los resultados de dicho tratamiento*»; y, «*c) analizar los datos PNR con el fin de actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave*». Artículo 6, apartado 2, letras b) y c), de la Directiva *PNR*.

relacionadas con el acceso[1031] y la utilización[1032] posterior de los datos conservados. Los datos del *PNR* sólo deben ser transferidos, almacenados y analizados por una entidad específicamente creada, la UIP, y el acceso a todo el conjunto de datos del *PNR*, que permite la identificación directa, sólo se transferirán a las autoridades encargadas de hacer cumplir la ley bajo condiciones muy estrictas y limitadas después del período inicial de almacenamiento.

115. El registro, en particular, de acuerdo con la Comisión Europea que lo ha propuesto, ayudará a prevenir ataques terroristas favoreciendo la identificación de los terroristas y su trazabilidad. Este desafío, hace que los Estados miembros puedan intercambiar automáticamente la información[1033] sobre el resultado del tratamiento de los datos del *PNR* y podrán pedir datos adicionales a sus socios si lo necesitan para una investigación.

116. La "necesidad y la proporcionalidad de la recogida de los datos *PNR*" como una medida necesaria para luchar contra el terrorismo y otras formas de delincuencia grave es, en nuestra opinión, una de las cuestiones más controvertidas[1034] a las que se enfrenta la recogida y utilización de estos datos. Siguiendo la línea trazada por la jurisprudencia de los tribunales europeos, para determinar las limitaciones a los derechos fundamentales incluidas en la Directiva *PNR*, es necesario evaluar si son necesarias y proporcionadas. Tal y como se ha podido comprobar, recientemente se ha debatido sobre los derechos fundamentales y, en particular, los principios de proporcionalidad y necesidad, en el contexto de la sentencia del TJUE en el asunto *Digital Rights Ireland*. El Tribunal formuló una serie de requisitos[1035],

[1031] Nos referimos a los artículos 6, apartado 7, 10 (Condiciones de acceso de Europol a los datos PNR) y 13 (Protección de los datos de carácter personal) de la Directiva *PNR*.

[1032] Artículo 6, apartado 2, artículo 7 (Autoridades competentes), apartado 4, artículo 11 (Transferencias de datos a los terceros países), artículo 12 y artículo 13 de la Directiva *PNR*.

[1033] Artículo 9 (Intercambio de información entre Estados miembros), apartado 1, de la Directiva *PNR*. La UIP, que es la autoridad que tiene los datos, deberá transmitirlos, en función de cada caso, a las autoridades competentes de su propio Estado, a las UIP o autoridades competentes de otro Estado miembro e, igualmente, si se cumplen los requisitos previstos en la Directiva, a las autoridades competentes de terceros Estados. Tanto a nivel nacional como a nivel comunitario, la regla general es que la UIP está obligada a transmitir «*todos los datos PNR pertinentes y necesarios, o el resultado de su tratamiento*» respecto de las personas que hayan sido identificadas de conformidad con el artículo 6, apartado 2.

[1034] La cuestión se ha puesto de relieve entre los jefes de Estado y de Gobierno de la UE que han presionado al Parlamento Europeo para que apruebe la directiva que regulará los datos de los pasajeros aéreos y algunos eurodiputados, sobre todo de izquierda, que rechazaban la medida, cuestionando que la directiva no pasaría el requisito legal de las pruebas de necesidad y proporcionalidad y los tribunales lo tumbarían. A tal propósito, se pueden ver los videos del debate en el Parlamento Europeo en: EUROPEAN PARLIAMENT - Press Releases (2016), EU PNR: useful against terrorism, but privacy and proportionality worries remain, 13-04-2016.

[1035] En particular, declaró que la recopilación y el acceso de las autoridades competentes a los datos constituye una injerencia en el derecho a la intimidad y en el derecho a la protección de los datos personales establecido en los artículos 7 y 8 de la Carta. El Tribunal también afirmó que, para respetar el artículo 52 de la Carta, las limitaciones de los derechos antes mencionados deben estar previstas por la ley, respetar la esencia de esos

que sin duda son válidos para todas las medidas de seguridad que puedan interferir con la protección de los datos personales, especialmente si prevén la conservación de datos. Por consiguiente, la Directiva debe establecer "normas claras y precisas" que «*regulen el alcance y la aplicación de las medidas*» de que se trate y establezcan garantías mínimas para las personas cuyos datos se hayan conservado[1036].

117. Una cuestión importante surge de lo anterior: ¿la Directiva *PNR* para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, es un instrumento legítimo para combatir el terrorismo y otros delitos graves?

118. Más allá de las críticas a la privacidad de los pasajeros, un factor que cada Estado miembro tendrá que tener en cuenta en el momento de la aplicación interna de la Directiva *PNR*, el principal problema surge de que la Directiva lleva a utilizar los datos *PNR* como elementos de estudio para analizar los comportamientos potencialmente sospechosos de los individuos que no pueden atribuirse a ningún sistema existente de identificación (por ejemplo, los sujetos fichados por las autoridades judiciales), y prevenir con el uso de algoritmos biométricos y predictivos consecuencias de actividades terroristas o riesgos por la seguridad nacional[1037].

derechos y, con sujeción al principio de proporcionalidad, deben ser necesarias y realmente cumplir objetivos de interés general reconocidos por la Unión.

[1036] Véase, la sentencia del TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 54 y, por analogía, en lo que respecto al artículo 8 del CEDH, las citadas sentencias del TEDH, *Rotaru contra Romania*, apartados 57 a 59, y *S. and Marper contra Reino Unido*, apartado 99.

[1037] Una operación de minería de datos extensa para identificar estadísticamente un sujeto que pudiera ser más "predispuesto" a cometer delitos en el futuro. Aunque puede sonar como ciencia ficción, debe destacarse que esto es una realidad. Un programa similar, el "*ThinTread*", estuvo activo en los EE.UU. por iniciativa de la *NSA*, así como en el territorio chino, que se llevan a cabo actividades de vigilancia de la seguridad interna para evitar riesgos para la seguridad y el orden público en el Tíbet, a través del análisis del comportamiento de la capacidad a gran escala por delante de sus habitantes a través de tecnologías específicas de videovigilancia y el uso de grandes datos. Se trata de etiquetar estadísticamente a individuos basados en meros algoritmos (en la Directiva *PNR* se usa el término «*evaluación*», presente en el considerando 7 y artículo 6). El peligro de esta actividad es que los algoritmos son cajas negras ("*black box*"), de los que no conocemos el funcionamiento y por lo tanto no podemos cuestionar los resultados. El control, la verificación y la evaluación se basan en el uso indiscriminado de tecnologías sin preocuparse demasiado por los riesgos asociados. Sobre el programa "*ThinTread*", vid. Marina MESEGUER (2016), «ThinThread, el programa secreto que podría haber evitado los atentados del 11S», en *LaVanguardia.com*, 11/09/2016. Disponible en Internet: http://www.lavanguardia.com/internacional/20160911/41223154746/thinthread-programa-secreto-evitado-atentados-11s.html [consulta: 05 de octubre de 2016]. Sobre las cajas negras, vid. Frank PASQUALE (2015), *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts; London, England, Harvard University Press, págs. 320.

119. Más crítico ha sido el SEPD[1038], Giovanni Buttarelli, que rechaza la Directiva *PNR*, identificándola «*suscettibile di una censura da parte della Corte di Giustizia UE*», ya que viola el principio de proporcionalidad consagrados en los Tratados de Unión y definiendo la medida «*un infortunio legislativo*»[1039]. La falta de mención a la protección de los derechos fundamentales en la Directiva *PNR* suscita preocupación por su repercusión en los derechos fundamentales y cuestiona si dicha técnica es realmente indispensable para abordar eficazmente la delincuencia grave y el terrorismo[1040].

120. Por el contrario, los ataques que se llevaron a cabo, sobre todo en aquel periodo, en Bélgica y Francia, han demostrado que la información necesaria sobre los terroristas estaba ya disponible para todas las autoridades y que el *PNR* no habría añadido nada. Los vuelos ya son trazables y ya existe la posibilidad de identificar los "*foreign fighters*", según el cual el resultado de «*troppe informazioni equivale a nessuna informazione*»[1041]. Hubiera sido mejor fomentar el intercambio y análisis de la información.

121. También resulta criticable el *modus operandi* de la recogida de datos: todo se perfila para ver si hay algún comportamiento anormal y no según categorías. No es tanto un problema de la protección de la privacidad sino de legitimidad constitucional de la norma con respecto de los Tratados del UE[1042]. A este respecto, la jurisprudencia del TJUE y del

[1038] Ya en su Dictamen de 2011, el SEPD recordaba que el desarrollo de dicho sistema plantea graves problemas de transparencia y proporcionalidad y que podría conducir a una evolución hacia una sociedad de vigilancia. *Cfr*. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011: núms. 16, 17 y 19). También RESUMEN EJECUTIVO DEL SEGUNDO DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2015: núms. 62 a 66).

[1039] Entrevista del Supervisor Europeo de Protección de Datos, «Garante privacy Ue, Pnr è infortunio normativo. Buttarelli, misura costosissima e richiede tempi semi-biblici», en *Ansa.it*, 14 aprile 2016. Disponible en Internet: http://www.ansa.it/europa/notizie/rubriche/altrenews/2016/04/14/garante-privacy-ue-pnr-e-infortunio-normativo_d9014be4-028e-477a-9479-18cc06f72d51.html [consulta: 15 de junio de 2016].

[1040] Los derechos en juego incluyen el derecho a la privacidad (artículo 7 de la CDFUE), el derecho a la protección de datos (artículo 8 de la CDFUE) y, también el derecho a la no discriminación (artículo 21 de la CDFUE), siendo una discriminación la prohibición de procesar datos sensibles con arreglo a la norma en examen y, en caso de ampliación de la Directiva relativa a los pasajeros europeos a los vuelos intracomunitarios, una discriminación del derecho a la libre circulación, que sólo podrán restringirse por razones de orden público o de seguridad pública, siempre que las restricciones respeten el principio de proporcionalidad.

[1041] «Garante privacy Ue, Pnr è infortunio normativo. Buttarelli, misura costosissima e richiede tempi semi-biblici», en *Ansa.it*. Los jueces que tienen una larga experiencia en investigaciones de terrorismo han expresado que hubieran preferido algo más inmediato, en lugar de una medida como el *PNR* que lleva muchos años y muchos miles de millones para ser implementado. Para la ejecución se requerirá enormes bases de datos y para la armonización de las normas y las normas de desarrollo se llevará tiempos semi-bíblicos, sólo pensamos cuántos años fueron necesarios para desarrollar el Sistema de Información de Schengen.

[1042] Se recordará que el artículo 52 de la CDFUE prevé que toda limitación de los derechos previstos en los artículos 7 y 8 de la CDFUE debe estar "prevista por la ley y respetar el contenido esencial de dichos derechos y libertades". «*Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás*».

TEDH confirman que la norma debe ser suficientemente precisa para indicar a los ciudadanos en qué circunstancias y en qué condiciones las autoridades públicas tienen facultades de conservar la información de su vida privada y el uso que se hace de ellas[1043]. En esta dirección, cualquier sistema de recogida de datos de carácter personal no puede extenderse a todo el mundo, menos a las personas contra las que no hay la más mínima sospecha de estar relacionadas con actividades delictivas. Es precisamente sobre la base de estos principios el TJUE, tal y como se ha podido comprobar, que se ha anulado la Directiva 2006/24/CE.

122. Estas críticas han sido avaladas también por el TJUE en su análisis sobre el Acuerdo de registro de pasajeros firmado por la Unión Europea y Canadá en 2014. Recordemos que incluso antes de la Directiva *PNR* Europa tuvo acuerdos de transferencia de datos *PNR* con Australia, EE.UU. y Canadá. Este último Acuerdo fue enviado al TJUE para un análisis preliminar[1044] que se pronunció el 26 de junio de 2017 de forma desfavorable al Acuerdo, al considerar que en su forma actual es incompatible con la legislación europea[1045]. El proyecto de Acuerdo UE-Canadá es incompatible con el artículo 7 de la CDFUE, que garantiza el derecho al respeto de la vida privada y el artículo 8 sobre el derecho a la protección de datos personales[1046]. Esta es la primera vez que el TJUE decide sobre la compatibilidad de un

[1043] En particular *vid*. la sentencia *Rotaru contra Romania*, apartados 52 y 55.

[1044] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2014, sobre la solicitud al Tribunal de Justicia de un dictamen sobre la compatibilidad con los Tratados del Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros, (2014/2966(RSP)). Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0058+0+DOC+XML+V0//ES [consulta: 15 de junio de 2016].

[1045] COURT OF JUSTICE OF THE EUROPEAN UNION - Press Release (2017), The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form, núm. 84/17, Luxembourg, 26 July 2017. Disponible en Internet: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf [consulta: 06 de septiembre de 2017]. También el Abogado General del TJUE, Paolo Mengozzi, se había pronunciado anteriormente sobre la proporcionalidad del Acuerdo *PNR* entre la Unión Europea y Canadá, a petición del Parlamento Europeo. En sus conclusiones, el Abogado General señala que el Acuerdo, no se puede celebrar en su forma actual. Varias «*disposiciones del proyecto de Acuerdo*», de hecho, «*son contrarias a los derechos fundamentales de la UE*». El Abogado General llega a estas conclusiones basadas en las lecciones aprendidas de los juicios *Digital Rights Ireland* y *Schrems* (sobre esta sentencia, ver *infra*). En su opinión, es necesario seguir el camino trazado en estas sentencias y presentar el acuerdo previsto a un «*estricto control*» sobre «*el derecho al respeto de la vida privada y familiar y el derecho a la protección de datos personales*». De hecho, es necesario que, en un momento en que las tecnologías modernas permiten a las autoridades públicas, en nombre de la lucha contra el terrorismo y la delincuencia transnacional grave, «*desarrollar métodos altamente sofisticados de vigilancia de la vida privada de los individuos y el análisis de sus datos personalmente*», el Tribunal se asegure de que las medidas propuestas, incluso en forma de acuerdos internacionales, reflejan una síntesis equilibrada entre la necesidad legítima de proteger la seguridad pública y que todos puedan disfrutar de un nivel alto de protección de su privacidad y sus datos. CONCLUSIONES DEL ABOGADO GENERAL Sr. Paolo Mengozzi, presentadas el 8 de septiembre de 2016, Dictamen 1/15, Solicitud de dictamen presentada por el Parlamento Europeo.

[1046] Para profundizar el tema *vid*. Wojciech R. WIEWIÓROWSKI (2017: 185 y ss.); Matteo LEFFI (2017a), «L'Accordo PNR tra Canada e UE non prende il volo. Nota sul parere della Corte di giustizia europea a proposito del trasferimento dei dati del codice di prenotazione», en *media laws*. Disponible en Internet:

proyecto de Acuerdo con la CDFUE; y por tercera vez[1047], que el TJUE afirma que la recopilación indiscriminada y la retención de datos de los individuos es ilegal en la Unión Europea. La injerencia en los derechos fundamentales que trajo el Acuerdo previsto "persigue un objetivo de interés general", a saber, "la seguridad pública y la lucha contra el terrorismo y el delito transnacional grave". Sin embargo, el TJUE recordó que, para estar justificada, una interferencia debe limitarse a «*lo estrictamente necesario para lograr el objetivo perseguido*».

123. En conclusión, según el TJUE, el intercambio de datos entre la UE y Canadá no cumple los criterios de necesidad y proporcionalidad esenciales para restringir el derecho fundamental de los ciudadanos a la protección de datos personales[1048]. En consecuencia, el Tribunal considera que el Acuerdo debe: "determinar de manera más clara y precisa algunos de los datos *PNR* que deben transferirse; disponer modelos y criterios utilizados para el tratamiento automatizado de datos *PNR* específicos, fiables y no discriminatorios; disponer que las bases de datos utilizadas se limitarán a las utilizadas por el Canadá en relación con la lucha contra el terrorismo y la delincuencia transnacional grave; disponer que las autoridades canadienses sólo puedan divulgar datos *PNR* a las autoridades gubernamentales de un país no comunitario si existe un acuerdo entre la Unión Europea y ese país equivalente al acuerdo previsto o una decisión de la Comisión Europea en este ámbito; prever un derecho de notificación individual para los pasajeros aéreos en caso de utilización de datos *PNR* que les conciernen durante su estancia en Canadá y después de su vuelta y en caso de que se divulguen dichos datos a otras autoridades o/a particulares; y, por último, garantizar que la supervisión de las normas relativas a la protección de los pasajeros aéreos con respecto al

http://www.medialaws.eu/laccordo-pnr-tra-canada-e-ue-non-prende-il-volo-nota-sul-parere-della-corte-di-giustizia-europea-a-proposito-del-trasferimento-dei-dati-del-codice-di-prenotazione/; Mario MENDEZ (2017), «Opinion 1/15: The Court of Justice Meets PNR Data (Again!)», en *European Papers*, vol. 2, núm. 3, págs. 803-818; Chiara GRAZIANI (2018), «PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali», en *DPCE Online*, vol. 33, núm. 4, págs. 959-966. Disponible en Internet: http://www.dpceonline.it/index.php/dpceonline/article/view/474 [documentos consultados: 11 de enero de 2018].

[1047] La primera fue en 2014, anulando la Directiva "*Data Retention*"; la segunda en 2016, con la sentencia *Tele2 Sverige-Watson* (vid. más adelante, apartado 3 del presente Capítulo).

[1048] Los datos *PNR* se describen como potencialmente útiles para fines definidos como prevención, investigación y represión del terrorismo y delitos graves. El Tribunal observa que la transferencia de datos sensibles (raza, etnia, política, religión, salud, sexo, *etc*.) a Canadá no parece estar suficientemente justificada y no existen criterios adecuados para regular el uso de los datos en territorio canadiense, evitando así posibles abusos. Lo que sugiere el Tribunal es que la transferencia sea subordinada al orden de un magistrado o un organismo independiente, salvo en los casos de urgencia. Marina CASTELLANETA (2017), «Trasferimento dei codici di prenotazione: Lussemburgo boccia il progetto di accordo UE-Canada», en *marinacastellaneta.it*, luglio 28. Disponible en Internet: http://www.marinacastellaneta.it/blog/trasferimento-dei-codici-di-prenotazione-lussemburgo-boccia-il-progetto-di-accordo-ue-canada.html [consulta: 07 de septiembre de 2017].

tratamiento de sus datos *PNR* sea llevada a cabo por una autoridad supervisora independiente"[1049].

124. El Tribunal también señaló que el Acuerdo debía celebrarse sobre la base de los artículos 16 del TFUE (protección de datos personales) y 87 (cooperación judicial en materia penal y cooperación policial)[1050].

125. Este dictamen del TJUE resulta fundamental[1051], especialmente en un momento histórico en el que varios países europeos están presionando para la aprobación de normas restrictivas de las libertades por la creciente alarma ante la amenaza terrorista que no deja de expandirse dentro de Europa[1052]. Con esta decisión, el TJUE de hecho fija un marco de la política de seguridad común europea, ya que el Acuerdo para un *PNR* entre la UE y Canadá, firmado en 2014, representa la base de los nuevos *PNR* (como por ejemplo de los EE.UU. y Australia). Un problema más, visto que sobre el *PNR* entre Unión Europea y Canadá el Consejo de la UE adoptó la Propuesta de Directiva *PNR* de la UE[1053]. No parece absurdo descartar que los Acuerdos existentes también puedan revisarse a raíz del dictamen, creando

[1049] COURT OF JUSTICE OF THE EUROPEAN UNION - Press Release (2017). En su versión original en inglés: «*Accordingly, the Court considers that the agreement should: determine in a more clear and precise manner certain of the PNR data to be transferred; provide that the models and criteria used for the automated processing of PNR data will be specific, reliable and non-discriminatory; provide that the databases used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime; provide that PNR data may be disclosed by the Canadian authorities to the government authorities of a non-EU country only if there is an agreement between the European Union and that country equivalent to the envisaged agreement or a decision of the European Commission in that field; provide for a right to individual notification for air passengers in the event of use of PNR data concerning them during their stay in Canada and after their departure from that country, and in the event of disclosure of that data to other authorities or to individuals; guarantee that the oversight of the rules relating to the protection of air passengers with regard to the processing of their PNR data is carried out by an independent supervisory authority*».

[1050] El Parlamento Europeo, en su Resolución de 25 de noviembre de 2014, preguntó si el Acuerdo con Canadá «*debe basarse jurídicamente en los artículos 82 del TFUE y 87 del TFUE (cooperación judicial en materia penal y cooperación policial) o bien en el artículo 16 del TFUE (protección de los datos de carácter personal)*». A este respecto, el Abogado General en su conclusión contestaba que «*el Acuerdo debe celebrarse a la vez sobre la base de los artículos 16 del TFUE y 87 del TFUE. En efecto, el Acuerdo previsto persigue dos objetivos indisociables y de igual importancia (por una parte, el de la lucha contra el terrorismo y los delitos graves de carácter transnacional - que se desprende del artículo 87 TFUE - y, por otra parte, el de la protección de los datos de carácter personal - que se desprende del artículo 16 del TFUE)*». COURT OF JUSTICE OF THE EUROPEAN UNION - Press Release (2017).

[1051] EUROPEAN COMMISSION - Statement (2017), EU-Canada PNR agreement: Commission statement on the Opinion of the European Court of Justice, Brussels, 26 July 2017. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-17-2105_en.htm [consulta: 08 de septiembre de 2017].

[1052] Por lo tanto, parece que se ha repetido el caso de 2012 donde el Parlamento Europeo votó por razones políticas en favor de un Acuerdo *PNR* EU-EE.UU. que no cumplía con los requisitos que el mismo Parlamento había exigido anteriormente. Si entonces las amenazas estadounidenses fueran a obligar a muchos parlamentarios a cambiar su voto, en esta ocasión hubo presiones políticas por parte de los Estados miembros causadas por los temores que se habían apoderado del viejo continente frente a los atentados de Francia y Bélgica.

[1053] Claudi PÉREZ (2017), «La justicia europea falla contra el registro de pasajeros con Canadá y siembra dudas sobre el europeo», en *El País*, 26 jul.

aún más incertidumbre y brechas adicionales en el sistema de protección de datos a favor de una mayor seguridad pública.

3. La anulación del Acuerdo sobre la transferencia de datos a EE.UU. ("*Safe Harbour*"): El asunto *Schrems*

126. La jurisprudencia "histórica"[1054] con la que el TJUE está definiendo el contenido del derecho a la tutela de los datos personales frente a las medidas de seguridad y orden público se inicia con la sentencia *Digital Rights Ireland* de 2014 analizada en el apartado anterior, que tiene como resultado una reconfiguración de las relaciones con EE.UU., defendiendo el derecho a la privacidad frente a los usos y abusos del procesamiento de datos en la Web, con particular referencia a la transferencia de datos personales a garantía de la seguridad pública desde países miembros de la UE hacia EE.UU.

127. Al igual que el fallo analizado en el apartado precedente, en su sentencia de 6 de octubre de 2015 en el asunto C-362/14[1055], el TJUE anuló la Decisión 2000/520/CE de la Comisión Europea, de 26 de julio de 2000 (*infra*), que reconocía, en el contexto del llamado régimen de "Puerto Seguro" (en inglés, "*Safe Harbour*"), un nivel de protección adecuado de los datos personales en EE.UU.[1056]. Esta sentencia, que aplica la Directiva 95/46/CE sobre

[1054] En Marco BASSINI, Oreste POLLICINO (2015), «La Corte di giustizia demolisce il *safe harbor* e ridisegna i confini del diritto alla privacy in ambito transnazionale», en *Diritto24 - Il Sole 24 Ore*, 7 ottobre. Disponible en Internet: http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2015-10-07/la-corte-giustizia-demolisce-safe-harbor-e-ridisegna-confini-diritto-privacy-ambito-transnazionale-153618.php [consulta: 11 de enero de 2016].

[1055] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, asunto C-362/14, sentencia de 6 de octubre de 2015.

[1056] La decisión despertó gran interés en la doctrina y hubo muchos comentarios. *Vid*. en particular, Alessandro DEL NINNO (2015), «Invalidità della Decisione Safe Harbour per il trasferimento dei dati verso gli USA: l'impatto pratico sulla esportazione dei dati personali», en *Diritto e Giustizia*. Disponible en Internet: http://www.dirittoegiustizia.it/news/17/0000075868/Invalidita_della_Decisione_Safe_Harbour_per_il_trasferimento_dei_dati_verso_gli_USA_l_impatto_pratico_sulla_esportazione_dei_dati_personali.html [consulta: 25 de enero de 2016]; Ana I. MENDOZA LOSANA (2015), «Transferencias internacionales de datos personales: Estados Unidos no es un puerto seguro, pero tampoco una isla inalcanzable», en *Centro de Estudios de Consumo (C.E.S.C.O.) Universidad de Castilla-La Mancha*, págs. 18. Disponible en Internet: http://blog.uclm.es/cesco/files/2015/10/Transferencias-internacionales-de-datos-personales_Estados-Unidos-no-es-un-puerto-seguro-pero-tampoco-una-isla-inalcanzable.pdf [consulta: 21 de enero de 2016]; Serena CRESPI (2015b), «La tutela dei dati personali UE a seguito della sentenza Schrems», en *Eurojus Centro di Eccellenza Jean Monnet presso l'Università degli Studi di Milano*. Disponible en Internet: http://www.eurojus.it/la-tutela-dei-dati-personali-ue-a-seguito-della-sentenza-schrems/ [consulta: 30 de diciembre de 2015]; Pietro FALLETTA (2015), «La Corte di Giustizia, ancora una volta, contro le multinazionali del Web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14)», en *federalismi.it*, núm. 24, págs. 11. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=31041 [consulta: 30 de diciembre de 2015];

la protección de los datos personales, asestó un duro golpe a 15 años de transferencias de datos personales a los EE.UU. con consecuencias, de no poca importancia, también en las relaciones de confianza entre Bruselas y Washington. En la práctica, como veremos, la sentencia ha supuesto la renegociación de un Acuerdo que sustituye al viejo régimen de "Puerto Seguro", con el nuevo "*Privacy Shield*" de 2016, con lo que extiende a este ámbito de la relación transatlántica el impacto vinculante de la doctrina del TJUE sobre los derechos de la CDFUE.

3.1. El background: las transferencias de datos entre EE.UU.-EU ("Safe Harbour")

128. Antes de examinar el contenido de la sentencia, se hace necesario explicar el elemento central sobre el que se basa la sentencia: el "*Safe Harbour*".

129. El intercambio de datos entre los EE.UU. y la UE es el más intenso que existe a nivel mundial. Sin embargo, ha sido difícil establecer un marco regulatorio entre estos dos actores, ya que los intereses comerciales no son los únicos que se han tenido en cuenta a la hora de concluir acuerdos internacionales. En el ámbito de la seguridad, la UE y los EE.UU. también han creado sinergias estrechas desde hace tiempo y, en este sentido, se han aprobado varios acuerdos internacionales desde que ocurrieron los atentados del 11 de septiembre de 2001.

130. Los EE.UU. iniciaron en 1998 las negociaciones con la UE para conseguir una declaración de adecuación del nivel de protección de datos personales en la trasferencia de datos personales entre los países[1057]. En el momento en que dieron comienzo las negociaciones entre la UE y el Departamento de Comercio de EE.UU., ambas partes tenían posturas bastante distanciadas[1058]. El Departamento de Comercio de EE.UU. publicó el 21 de julio de 2000 un documento con los "Principios de Puerto Seguro" ("*Safe Harbour*

Raffaele BIFULCO (2016), «La sentenza Schrems e la costruzione del diritto europeo della privacy», en *Giurisprudenza costituzionale*, núm. 1, págs. 289-307.

[1057] Documents and Public Comments Provided through the Duration of the Safe Harbor Negotiations (November 1998 - June 2000), June 9, 2000.

[1058] Por ejemplo, la Comisión Federal de Comercio de EE.UU. (*Federal Trade Commission - FTC*) era más favorable a la autorregulación por la industria, así como el mejor método para otorgar protección de los datos personales con el menor impacto para el desarrollo económico. Por lo contrario, la UE defendía firmemente la legislación comprehensiva y detallada en materia de protección de datos. *Vid*. FEDERAL TRADE COMMISSION - press releases (1999), "Self-Regulation and Privacy Online", FTC Report to Congress, July 13, 1999. Disponible en Internet: https://www.ftc.gov/news-events/press-releases/1999/07/self-regulation-and-privacy-online-ftc-report-congress [consulta: 04 de enero de 2016]; Solveig SINGLETON (1999), «Privacy and Human Rights: Comparing the United States to Europe», en *Cato Institute White Paper*. Disponible en Internet: https://www.cato.org/publications/white-paper/privacy-human-rights-comparing-united-states-europe [consulta: 15 de julio de 2016].

Principles"), acompañado de las preguntas más frecuentes (*FAQ - Frequently Asked Questions*) con orientaciones sobre cómo aplicar dichos principios[1059].

131. Tras largas negociaciones[1060], el 26 de julio de 2000 la UE y EE.UU. llegaron a un Acuerdo denominado principios de "Puerto Seguro" - Decisión de la Comisión 2000/520/CE[1061] (en adelante, Decisión "Puerto Seguro") - sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. En el artículo 1, apartado 1, de la Decisión "Puerto Seguro", la Comisión manifestaba que esos principios, aplicados de conformidad con la orientación que proporcionan las *FAQ*, «*garantizan un nivel adecuado de protección de los datos personales*» transferidos desde la Unión a entidades establecidas en EE.UU.

[1059] Estos últimos, «*se formularon en consulta con la industria y opinión pública, para facilitar el comercio y las transacciones*» entre EE.UU. y la UE. Por un examen de los principios "*Safe Harbour*", *vid*. María ÁLVAREZ CARO y Miguel RECIO GAYO (2015), «Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU. y la UE», en *Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense Facultad de Derecho*, Papeles de Derecho Europeo e Integración Regional, núm. 25, págs. 26. Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2015-06-15-Binder218.pdf [consulta: 26 de enero de 2016]; Giorgio RESTA, Vincenzo ZENO-ZENCOVICH (2016), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, RomaTrE-Press, págs. 373. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/PTD [consulta: 03 de septiembre de 2016].

[1060] Entre 1998 y 1999, el Departamento de Comercio de EE.UU. remitió a la UE varias propuestas o esquemas de autorregulación y todos ellos fueron criticados por el Grupo de Trabajo, debido a la falta de eficacia y su incapacidad de proteger adecuadamente la privacidad de los ciudadanos europeos basándose en las disposiciones de la Directiva europea de 1995. *Vid*. GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (1999), Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti, 5092/98/EN/finale, WP 15, adottato dal Gruppo di Lavoro il 26 gennaio 1999. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp15_it.pdf [consulta: 04 de septiembre de 2016]. En mayo de 2000 el Grupo de Trabajo emitió otro dictamen sobre el nivel adecuado de protección de datos en las transferencias internacionales de datos, con especial atención a las negociaciones "*Safe Harbour Principles*" entre EE.UU. y la UE, destacando en sus conclusiones que «*la resolución propuesta sobre la adecuación se refiere a un sistema que todavía no es operativo. A este respecto, el Grupo de trabajo se congratula de la cláusula de revisión que aparece en la propuesta de Decisión de la Comisión, que permitirá revisar las resoluciones sobre adecuación a la luz de la experiencia*». *Vid*. ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS (2000), Dictamen 4/2000 sobre el nivel de protección que proporcionan los "principios de puerto seguro", CA07/434/00/ES, WP 32, aprobado el 16 de mayo de 2000; Alfonso ORTEGA GIMÉNEZ (2007), «Transferencia internacional de datos de carácter personal: U.E. vs. EE.UU.», en *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, vol. 1, núm. 2, marzo, págs. 212 y ss. ISSN: 1886-6611.

[1061] DECISIÓN DE LA COMISIÓN, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C(2000) 2441] (Texto pertinente a efectos del EEE.), 2000/520/CE, *Diario Oficial de la Unión Europea*, L 215, 25.8.2000, págs. 7–47. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32000D0520 [consulta: 25 de enero de 2016].

132. Por lo tanto, «*se trataba de un sistema "eficaz" desde el punto de vista teórico y práctico*», ya que facilita «*un flujo estable e ininterrumpido de información asegurando un nivel adecuado permanente de protección*»[1062]. Los principios incluidos en el régimen de "Puerto Seguro" buscaban empoderar al sujeto, requiriendo que fuera informado sobre el fin para el que sus datos iban a ser usados, dándole la oportunidad de elegir si sus datos podían ser usados para finalidades distintas a las que en un principio justificaron su recogida, y permitiéndole el acceso a sus datos para corregirlos, enmendarlos o suprimirlos cuando fuera necesario. El Departamento de Comercio de EE.UU. y la Comisión Federal de Comercio de los EE.UU. eran los responsables de la aplicación del sistema de "Puerto Seguro" en su país.

133. El sistema de principios de "Puerto Seguro"[1063], aunque ha sido criticado[1064], presentaba algunas ventajas, teniendo en cuenta que: «*constituía un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la privacidad y para la transferencia internacional de datos de carácter personal entre la UE y los EE.UU.*»; permitía «*la aprobación automática por todos los Estados miembros de la UE de las transferencias internacionales de datos de carácter personal con destino a los EE.UU.*» sustituyendo a «*las legislaciones internas de cada uno de los Estados miembros de la UE*»[1065].

[1062] Alfonso ORTEGA GIMÉNEZ (2014a), «Algunas claves en las relaciones entre los EEUU y la UE sobre transferencias de datos de carácter personal. El acuerdo de Puerto Seguro», en *Revista TELOS (Cuadernos de Comunicación e Innovación)*, Madrid, núm. 97, febrero-mayo.

[1063] *Vid*. *amplius*, Alicia CHICHARRO LÁZARO (2015), «La transcendencia práctica del caso Facebook en relación con la transferencia masiva de datos personales desde la Unión Europea a Estados Unidos», en Concha MATEOS MARTÍN, Francisco Javier HERRERO GUTIÉRREZ (coords.), *La pantalla insomne*, Cuadernos Artesanos de Comunicación, núm. 90, pág. 1867 y ss. Disponible en Internet: http://www.revistalatinacs.org/15SLCS/libro-colectivo-2015.html [consulta: 27 de julio de 2016].

[1064] Es importante señalar los riesgos del sistema estadounidense, en particular en lo que se refiere a la formación de "archivos gubernamentales" que contradicen la protección de los derechos fundamentales garantizados por la Unión Europea, *vid*. Solveig SINGLETON (1999). También, subrayando los aspectos críticos de "*Safe Harbor*" en términos de efectividad e implementación, vid. John T. SOMA, Stephen D. RYNERSON, and Britney D. BEALL-EDER (2004), «An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor», en *Texas International Law Journal*, vol. 39, págs. 171-214. Disponible en Internet: http://www.tilj.org/content/journal/39/num2/Soma-Rynerson-Beall-Eder171.pdf [consulta: 23 de agosto de 2016]; Stephen J. KOBRIN (2004), «Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance», en *Review of International Studies*, núm. 30, págs. 111-131. Disponible en Internet: https://mgmt.wharton.upenn.edu/profile/1334/research [consulta: 25 de julio de 2016]; Chris CONOLLY (2013), «EU/US Safe Harbour - Effectiveness of the Framework in relation to National Security Surveillance», en *Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens"*, Strasburgo, págs. 8; Jeff CHESTER (2014), «CDD Files Complaint on U.S./EU Safe Harbour for Data Privacy at FTC/Filing Reveals Failure of U.S. Agreement to Protect European Privacy», en *Centre for Digital Democracy*.

[1065] Alfonso ORTEGA GIMÉNEZ (2014a).

134. En su aplicación, las empresas que quisieran adherirse a este sistema debían «*presentar una carta de autocertificación ante el Departamento de Comercio*» de EE.UU., en la que «*manifieste su adhesión a los principios y FAQ, así como indicando, en particular, los datos de identificación de la entidad solicitante, una descripción de su actividad en lo relativo a la información personal recibida de la UE y una descripción de su política de protección de datos de carácter personal*»[1066]. El sistema de principios de "Puerto Seguro" se configuraba, entonces, «*como un programa voluntario*», no vinculante, «*basado en la autocertificación y en la autoevaluación, que se ofrece a las entidades estadounidenses con el fin de obtener, respecto de los datos personales recibidos desde la UE, una presunción de adecuación a la protección exigida en el ámbito europeo, que permite asegurar de manera permanente la legitimidad de las transferencias internacionales de datos de carácter personal*»[1067].

135. La entonces vicepresidenta de la Comisión Europea, Viviane Reding, y el Secretario de Comercio de los EE.UU., John Bryson, en 2012 publicaron una declaración conjunta sobre la privacidad[1068], reconociendo que, si bien los regímenes reguladores pueden diferir entre los EE.UU. y la UE, los principios comunes de ambos sistemas proporcionan una base para avanzar en el diálogo para resolver los desafíos compartidos de la vida privada en un interés mutuo. Pero un año después, la misma vicepresidenta de la Comisión Europea declaró, en el Consejo de Justicia de Vilnius, que el Acuerdo "*Safe Harbor*" puede no ser

[1066] Alfonso ORTEGA GIMÉNEZ (2014a). Las empresas que se adhieren a este Acuerdo se comprometen a gestionar los datos personales conforme a los principios del Acuerdo y disponen de una presunción de adecuación al nivel de protección exigido por la Directiva 95/46/CE. Los «*principios de "Puerto Seguro", que se configuran como mínimos para cualquier política privada de protección de datos de carácter personal, son los siguientes*»: notificación; opción; transferencia ulterior; seguridad; integridad de los datos; acceso; aplicación. *Vid*. ampliamente, Decisión de la Comisión 2000/520/CE. Sitio web "Puerto Seguro": *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*: https://2016.export.gov/safeharbor/index.asp.

[1067] Alfonso ORTEGA GIMÉNEZ (2014a). Damon GREEN (2011), «Safe Harbor-a framework that works», en *International Data Privacy Law*, vol. 1, issue 3. Disponible en Internet: https://doi.org/10.1093/idpl/ipr010 [consulta: 05 de agosto de 2016]. Las autoridades alemanas de protección de datos emitieron una decisión solicitando a las empresas que trasladan datos de Europa a los EE.UU. comprobar activamente que las empresas en los EE.UU. importan datos cumpliendo realmente con los principios de privacidad "*Safe Harbor*". La empresa exportadora de datos tiene que obtener evidencia de que las autocertificaciones "*Safe Harbor*" existen y que sus principios son cumplidos. La empresa exportadora debe aclarar al menos si la certificación "Puerto Seguro" del importador sigue siendo válida: «(…) *the company exporting data has to obtain evidence that the Safe-Harbor-self-certifications exist and that their principles are complied with. The exporting company has to clarify at least whether the importer's Safe-Harbor-certification is still valid*». *Vid*. Decision by the supreme supervisory authorities for data protection in the nonpublic sector on 28/29, April 2010 in Hannover [revised version of 23 August 2010].

[1068] EUROPEAN COMMISSION - Press Release (2012), EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, Memo/12/192, Brussels, 19 March 2012. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-12-192_en.htm?locale=en [consulta: 06 de agosto de 2016].

tan seguro, podría ser una «*loophole*»[1069] (escapatoria) para las transferencias de datos, ya que permitía transferencias de datos de la UE a las compañías estadounidenses, donde los estándares son más bajos que los europeos. La Comisaria Reding anunció una evaluación profunda del Acuerdo de "Puerto Seguro".

136. Tras la divulgación por parte de algunos medios de comunicación del escándalo "*Datagate*" (con especial referencia a los casos "*PRISM*" y "*Tempora*", y otros programas similares de vigilancia actuados también por EE.UU.), las instituciones europeas adoptaron una serie de iniciativas para analizar el alcance real de algunos programas de inteligencia utilizados por los EE.UU. y por algunos Estados miembros de la UE (ej. Reino Unido). Por otra parte, el «*acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos*» a EE.UU. por entidades con certificación de "Puerto Seguro" suscitó «*serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país*»[1070]. A raíz de estas revelaciones sobre los programas de vigilancia de los EE.UU., las autoridades alemanas de protección de datos expresaron su profunda preocupación de que existe una probabilidad sustancial de que se violen los principios de las decisiones de la Comisión y señaló que las compañías que envían datos personales a los EE.UU. son responsables de estos datos. El documento concluye que todo el mundo debe por tanto tener interés en garantizar que los flujos de datos personales no estén sujetos a una vigilancia a gran escala por parte de los servicios de inteligencia[1071].

137. Poco tiempo después, el 27 de noviembre de 2013, la Comisión Europea propuso 13 recomendaciones para mejorar y fortalecer el régimen de "Puerto Seguro"[1072], sobre la base

[1069] EUROPEAN COMMISSION - Memo (2013a), Informal Justice Council in Vilnius, Brussels, 19 July 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-710_en.htm [consulta: 08 de agosto de 2016].

[1070] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM/2013/0847 final, 27/11/2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52013DC0847 [consulta: 13 de agosto de 2016].

[1071] «*There is a substantial likelihood that the principles in the Commission's decisions are being violated.* (…) *Companies that send personal data to the U.S. bear the responsibility for these data. Like everyone in Germany, they must therefore have an interest in ensuring that personal data flows are not subject to large-scale surveillance by intelligence services*». *Cfr*. Die Landesbeauftragte für Datenschutz und Informationsfreiheit - Press release, Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe, Bremen/Bremerhaven, 24 July 2013.

[1072] «*1. Las entidades autocertificadas deberán hacer públicas sus políticas de protección de la vida privada. 2. Las políticas de protección de la vida privada que figuren en los sitios web de las entidades autocertificadas deberán incluir siempre un vínculo al sitio del Departamento de Comercio dedicado al puerto seguro, que contiene una lista de todos los miembros «actualizados» del sistema. 3. Las entidades autocertificadas deberán hacer públicas las condiciones de respeto de la vida privada de todo contrato que celebren con subcontratistas, como los servicios de computación en nube. 4. El sitio web del Departamento de Comercio deberá indicar claramente todas las entidades que actualmente no son miembros del sistema. 5. Las políticas de protección*

de un análisis exhaustivo y consultas con las empresas[1073]. La Comisión pidió a las autoridades de EE.UU. que identificasen soluciones para mediados de 2014, a partir de las cuales revisó el funcionamiento del sistema de "Puerto Seguro" basado en la aplicación de las 13 recomendaciones[1074].

138. El Parlamento Europeo solicitó, con un informe de la Comisión LIBE[1075], la suspensión del "Puerto Seguro" por falta de consistencia del Acuerdo en términos de seguridad para los ciudadanos europeos[1076]. El Parlamento reiteró la «*suspensión inmediata*» del Acuerdo de "Puerto Seguro", en los que se afirma que estos principios «*no proporcionan una protección adecuada a los ciudadanos de la UE*» e instando a los EE.UU. a proponer

de la vida privada que figuren en los sitios web de las entidades deberán incluir un vínculo a su proveedor de servicios de solución extrajudicial de litigios o al Panel de la UE. 6. Los servicios de solución extrajudicial de litigios deberán ser asequibles y estar fácilmente disponibles. 7. El Departamento de Comercio debe supervisar de manera más sistemática a los proveedores de servicios de solución extrajudicial de litigios en lo que respecta a la transparencia y la accesibilidad de la información que facilitan sobre sus procedimientos y sobre el seguimiento dado a las quejas. 8. Tras la certificación o la renovación de la certificación de las entidades, conviene someter a un porcentaje de ellas a investigaciones de oficio para comprobar el cumplimiento efectivo de sus políticas de protección de la vida privada (yendo más allá del mero control del cumplimiento de las exigencias formales). 9. Siempre que se constate un incumplimiento a raíz de una queja o una investigación, deberá someterse a la entidad a una investigación específica al cabo de un año. 10. Cuando existan dudas sobre el cumplimiento por parte de una entidad, o si hay quejas pendientes, el Departamento de Comercio deberá comunicarlo a la autoridad de protección de datos de la UE competente. 11. Hay que seguir investigando las afirmaciones falsas de adhesión a puerto seguro. 12. Las políticas de protección de la vida privada de las entidades autocertificadas deben incluir información sobre la medida en que la legislación estadounidense permite a las autoridades públicas recoger y tratar datos transferidos al amparo de puerto seguro. 13. Es importante que la excepción relativa a la seguridad nacional prevista en la Decisión de puerto seguro no se utilice más allá de lo estrictamente necesario o proporcionado». *Vid*. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE.

[1073] La Comisión Europea, desde el establecimiento del Acuerdo, destacaba que 3.246 compañías americanas habían suscrito el Acuerdo de forma voluntaria: «*By late-September 2013, the Safe Harbour had a membership of 3246 companies (an eight-fold increase from 400 in 2004)*». En EUROPEAN COMMISSION - Memo (2013c), Restoring Trust in EU-US data flows - Frequently Asked Questions, Brussels, 27 November 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm [consulta: 13 de agosto de 2016].

[1074] El Grupo de Trabajo confirmó las 13 recomendaciones de la Comisión Europea para mejorar el funcionamiento del sistema de "Puerto Seguro", en particular las recomendaciones 12 y 13. ARTICLE 29 DATA PROTECTION WORKING PARTY (2014b), Appendix: WP29 additional recommendations to strengthen personal data protection under the Safe Harbor Decision, Brussels, 10 April 2014. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf [consulta: 17 de agosto de 2016].

[1075] INFORME sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior, (2013/2188(INI)), 21 de febrero de 2014. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES [consulta: 18 de agosto de 2016].

[1076] Un mes antes, el 28 de enero de 2014, de nuevo la vicepresidenta de la Comisión Europea, Viviane Reding, explicaba que para que "*Safe Harbor*" sea totalmente manejable, los EE.UU. tendrán que darle servicio y que el "Puerto Seguro" tiene que ser fortalecido o será suspendido: «*Safe Harbour has to be strengthened or it will be suspended*». EUROPEAN COMMISSION - Press Release (2014), A data protection compact for Europe, CEPS/Brussels, 28 January 2014. Disponible en Internet: http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm [consulta: 18 de agosto de 2016].

nuevas normas de transferencia de datos personales que cumpliesen los requisitos de protección de datos de la UE[1077].

139. En este sentido, en paralelo al "Puerto Seguro", EE.UU. y UE, después de cuatro años de largas negociaciones, desde el 29 de marzo de 2011, llegaron, el 8 de septiembre de 2015, a un "Acuerdo marco sobre protección de datos" en el ámbito de la cooperación policial y judicial (*Data protection* "*Umbrella Agreement*") que tiene por objeto la protección de datos personales intercambiados entre la UE y los EE.UU. y las salvaguardias necesarias para la prevención, detección, investigación y enjuiciamiento de delitos, incluido el terrorismo[1078] (*amplius infra*).

3.2. Facebook y NSA: la transferencia de datos personales europeos en los EE.UU.

140. En la sentencia del TJUE, objeto de análisis recurrente, el Sr. Maximillian Schrems[1079], estudiante austriaco, era usuario de la red social *Facebook* desde 2008. *Facebook*, es de propiedad y de gestión *Facebook Inc*., con sede en Palo Alto, California. Con el fin de utilizar los servicios ofrecidos por la plataforma, cada usuario tiene necesariamente que firmar un contrato con la empresa *Facebook Ireland*, filial de *Facebook Inc*., ubicada en territorio irlandés. En particular, como ocurre con todos los usuarios que viven en la Unión Europea, la información suministrada a la plataforma es transferida, en su totalidad o en parte, a la sucursal irlandesa de *Facebook* en servidores ubicados en el territorio de los EE.UU. (California), donde se procesan.

141. El Sr. Schrems denunciaba ante la Autoridad Irlandesa de Protección de Datos (*Data Protection Commissioner*), a la luz de las revelaciones "*Datagate*" realizadas en 2013 por el analista Edward Joseph Snowden sobre las actividades de inteligencia de la Agencia de

[1077] PARLAMENTO EUROPEO - Notas de prensa (2014a), EE.UU. debe poner fin al espionaje masivo o afrontar las consecuencias, advierte el PE, 12-03-2014. Disponible en Internet: http://www.europarl.europa.eu/news/es/news-room/20140307IPR38203/ee.uu.-debe-poner-fin-al-espionaje-masivo-o-afrontar-las-consecuencias [consulta: 23 de agosto de 2016]. El 29 de octubre de 2015, el Parlamento adoptó una Resolución sobre el seguimiento de la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la vigilancia electrónica masiva de los ciudadanos de la UE (vid *infra*), en la que reiteraba su llamamiento en favor de la suspensión de la Decisión "Puerto Seguro" y del Programa de Seguimiento de la Financiación del Terrorismo.

[1078] EUROPEAN COMMISSION - Fact Sheet (2015b), Questions and Answers on the EU-US data protection "Umbrella agreement", Brussels, 8 September 2015. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm [consulta: 24 de agosto de 2016]. En junio de 2015, se promulgó en EE.UU. el *USA Freedom Act*, que modifica algunas disposiciones del *Patriot Act*, imponiendo nuevos límites a la recopilación de metadatos de los ciudadanos estadounidenses por medio de los sistemas de telecomunicación interceptados por parte de las agencias de inteligencia de los EE.UU.

[1079] Sobre los antecendentes, véanse Alicia CHICHARRO LÁZARO (2015: 1860 y ss.).

Seguridad Nacional estadunidense (*NSA*)[1080], que el derecho y la práctica de EE.UU. no proporcionaban una adecuada protección contra la vigilancia llevada a cabo por las autoridades públicas en los datos transferidos a ese país, requisito imprescindible para hacer legal la transferencia de datos a los EE.UU. Se ponen en discusión, por lo tanto, las transferencias de datos personales de *Facebook* Irlanda a *Facebook* EE.UU. frente a un acceso generalizado que las autoridades estadounidenses tendrían en estos datos.

142. A este respecto, el artículo 25 de la Directiva 95/46/CE establecía que la transferencia de datos a un tercer país puede tener lugar sólo si el tercer país garantiza un nivel adecuado de protección de datos. También de acuerdo con la Directiva, la Comisión Europea podía determinar que un tercer país, en consideración de su legislación interna o de sus compromisos internacionales, garantice un nivel adecuado de protección[1081]. En este sentido, mediante la Decisión "Puerto Seguro", la Comisión Europea reconoció un "*sui generis*"[1082] nivel de protección adecuado de los datos personales en EE.UU. denominado régimen de "Puerto Seguro" consistente en proclamar una serie de principios de protección de datos personales a los que las empresas estadounidenses podían suscribirse voluntariamente. Por último, según el artículo 28 de la Directiva 95/46/CE, cada Estado miembro designa una o más autoridades públicas responsables de la supervisión de la aplicación en su territorio de las disposiciones de aplicación de la Directiva adoptada por los Estados miembros.

[1080] Sobre los efectos del "*Datagate*" generado por las revelaciones de Edward Snowden, vid. Giorgio RESTA, Vincenzo ZENO-ZENCOVICH (2016: 23 y ss.).

[1081] Los artículos 25 y 26 de la Directiva 95/46/CE delineaban dos maneras diferentes para garantizar, a los datos personales de los ciudadanos europeos, estándares adecuados de protección: por un lado, los acuerdos entre importadores y exportadores de datos, del otro, las evaluaciones de adecuación. Cada uno de los parámetros señalados por la disposición deben ser evaluados periódicamente por la Comisión Europea, pena la anulación de la decisión. Gloria GONZÁLEZ FUSTER (2014a: 124-156). El nivel adecuado se «*evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos*». En particular, «*se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el tercer país de que se trate, así como las normas profesionales y las medidas de seguridad en vigor*». «*Si se comprueba que un tercer país no garantiza un nivel adecuado de protección, los Estados miembros impedirán que se le transfieran datos personales*». Por el contrario, de no existir tal reconocimiento de adecuación, cada transferencia de datos operada por una institución o empresa desde un Estado miembro a un país tercero deberá ser objeto de un contrato autorizado por la Autoridad nacional de Protección de Datos en el que, para cada transferencia internacional específica, se garantizará el cumplimiento de la normativa europea. Artemi RALLO LOMBARTE (2017: 605). Como excepción se señala que «*podrá efectuarse dicha transferencia a un país tercero que no garantice un nivel de protección adecuado*» cuando sea «*necesaria*» o legalmente exigida para la «*salvaguardia de un interés público importante*». Por tanto, la transmisión es ilícita, a menos que se den unas condiciones de licitud, que son la existencia de un nivel de protección adecuado en el Estado de destino o, en defecto de tal nivel, una de las excepciones enumeradas en la propia Directiva. Alicia CHICHARRO LÁZARO (2015: 1864).

[1082] Artemi RALLO LOMBARTE (2017: 605).

143. En primera instancia, la Autoridad Irlandesa de Protección de Datos (*Data Protection Commissioner*) desestimó la denuncia al considerarla infundada, en particular, sobre la base de que el régimen de transferencia "Puerto Seguro" garantizaba un nivel adecuado de protección para transferir los datos personales desde la UE a organizaciones ubicadas en los EE.UU. sobre la base de la documentación publicada por el Departamento de Comercio de EE.UU. También la *Data Protection Commissioner* declaraba que no tenía competencia para juzgar la adecuación de tal sistema, justificándolo en que estaba obligada por esta Decisión de la Comisión Europea por razón del principio de la supremacía del Derecho de la Unión sobre el derecho interno.

144. No satisfecho el Sr. Schrems, en segundo lugar, se dirigió al Tribunal Supremo de Irlanda (*High Court of Ireland*), para recurrir la decisión de la *Data Protection Commissioner*. El Tribunal Supremo de Irlanda, decidió suspender el procedimiento, y elevó al TJUE unas cuestiones prejudiciales sobre su interpretación[1083], para determinar si la Decisión 2000/520/CE de la Comisión de 26 de julio de 2000 producía el efecto de impedir que una autoridad nacional de control pueda decidir sobre un recurso con el que deniega que un país tercero no garantiza un nivel adecuado de protección y, si necesario, para suspender la transferencia de datos impugnados. En concreto, se plantea al TJUE dos cuestiones prejudiciales, que son las siguientes: «*1) En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE? 2) En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520?*»[1084].

3.3. La interpretación de la legalidad europea conforme a los derechos fundamentales por la CDFUE y su salvaguarda por autoridades de control

145. El primer aspecto que se trata por la sentencia del TJUE, invierte la intervención de las autoridades nacionales de control que tienen, frente a una Decisión de la Comisión

[1083] Alicia CHICHARRO LÁZARO (2015: 1862).
[1084] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 36.

Europea, la obligación de verificar la idoneidad del nivel de protección garantizada por el Estado tercero.

146. Después de enmarcar el papel de las autoridades de control[1085], el Tribunal señala que estos juegan un papel en la transferencia de datos a terceros países. La importancia concedida por los jueces de Luxemburgo a las autoridades de control nacional como entidades independientes[1086] no es nueva. El papel central de éstas en el sistema de protección de los datos personales de la UE no se refería únicamente en el artículo 8, apartado 3, de la CDFUE, sino es también la base de la sentencia *Digital Rights Ireland*[1087].

147. El TJUE, sobre las cuestiones prejudiciales, considera que la existencia de una Decisión de la Comisión en la que se declare que un tercer país garantiza un nivel adecuado de protección de los datos personales transferidos[1088], «(…) *no impide que una autoridad de control de un Estado miembro* (…) *pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado*». El Tribunal recuerda, en este sentido, que el derecho a la protección de datos personales garantizado por la Directiva 95/46/CE, que implica «*libertades fundamentales y, en particular, el derecho al respeto de la vida privada*» debe

[1085] Como se ha indicado anteriormente, el artículo 28, apartado 1, de la Directiva 95/46/CE imponía a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control del cumplimiento de las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de sus datos personales. Michele NINO (2015), «La Corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbour: la sentenza Schrems», en *SIDIBlog*, vol. 2. Disponible en Internet: http://www.sidiblog.org/2015/10/24/la-corte-di-giustizia-ue-dichiara-linvalidita-del-sistema-di-safe-harbour-la-sentenza-schrems/ [consulta: 19 de septiembre de 2016].

[1086] «*La garantía de independencia de las autoridades nacionales de control pretende asegurar un examen eficaz y fiable del respeto de la normativa en materia de protección de los datos personales. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades*». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 41.

[1087] Esa exigencia está expresamente contemplada en el Derecho primario de la Unión Europea, en particular del artículo 8, apartado 3, de la CDFUE y del artículo 16 del TFUE, apartado 2 y en las sentencias del TJUE (Gran Sala), *Comisión Europea contra República de Austria*, apartado 36 y *Comisión Europea contra Hungría*, asunto C-288/12, sentencia de 8 de abril de 2014, apartado 47. Vid. también en ese sentido, TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 68 y TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 40. Artemi RALLO LOMBARTE (2017: 607).

[1088] El Grupo de Trabajo, tomando en cuenta la Directiva y otros instrumentos internacionales sobre protección de datos, apuntó una serie de principios de contenido y de requisitos de procedimiento, cuyo cumplimiento pudiera considerarse la condición mínima para juzgar adecuada la protección. GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1998).

ser "necesariamente" interpretado «*a la luz de los derechos fundamentales protegidos*» por la CDFUE (artículos 7 y 8)[1089].

148. El Tribunal, confirmó el papel de las autoridades nacionales de control independiente, especialmente formulado para que ejerzan una vigilancia sobre el cumplimiento de las disposiciones relativas a la protección de las personas físicas con respecto al tratamiento de datos personales[1090]. Precisamente, el TJUE aclara el valor de esta tarea de comprobación y control en relación con las medidas puestas en marcha por los titulares del trato, para que ellas resulten eficaces y fiables. En este sentido, y en atención a esta finalidad se debe evaluar su actividad sobre la operación que consiste en la transferencia de datos personales por parte de un Estado miembro a un tercer país y constituye una forma de tratamiento perfectamente calificado como tal de acuerdo con los dictados del artículo 2, letra b), de la Directiva 95/46/CE[1091]. También señala que esas autoridades pueden actuar como otra forma de control ya que "no son enumeradas de forma exhaustiva" por el artículo 28, apartado 3, de la Directiva 95/46/CE[1092]. Por lo tanto, incluso aunque exista una Decisión de la Comisión Europea, "las autoridades nacionales de control deben ser capaces de

[1089] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 37 y 38. Véanse las sentencias del TJUE, *Österreichischer Rundfunk y otros*, apartado 68; *Google Spain*, apartado 68. La Directiva 95/46/CE, en su artículo 1 y considerandos 2 y 10, pretende garantizar «*no sólo una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas frente al tratamiento de los datos personales*», sino también «*un elevado nivel de protección de esas libertades y derechos fundamentales*». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 39.

[1090] La garantía de independencia de las autoridades nacionales de control «*se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales*». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 41.

[1091] En el sentido del artículo 2, letra b), de la Directiva 95/46/CE, por «*tratamiento de datos personales*» se identifica «*cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales*», y que comprende «*la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos*» de los datos personales del propio territorio nacional a un diferente Estado. *Vid*. TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 45. El Tribunal ha confirmado, en esencia, las conclusiones ya expresadas por el Abogado General Yves Bot. Las conclusiones del Abogado General se basaron en tres puntos esenciales: a) los sistemas de vigilancia masiva utilizados por los EE.UU. conducen a una injerencia en los derechos fundamentales de los ciudadanos de la UE en lo que respecta a su privacidad; b) el "*Safe Harbor*" no proporciona una protección adecuada a los ciudadanos de la UE frente a esta interferencia y es nula; c) la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000 no tiene por efecto impedir que una autoridad de control nacional investigue una denuncia en la que se alega que un país tercero no garantiza un nivel de protección adecuado de los datos de carácter personal y, en su caso, suspenda la transferencia de dichos datos. CONCLUSIONES DEL ABOGADO GENERAL Sr. Yves Bot, presentadas el 23 de septiembre de 2015, asunto C-362/14.

[1092] Así pues, esas autoridades disponen, en particular, «*de facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio,* (…) *están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales* (…)». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 43 y 47.

examinar, con total independencia, si la transferencia de datos de una persona a un tercer país cumple los requisitos de la Directiva 95/46/CE"[1093].

149. De acuerdo con el artículo 288 del TFUE, apartado cuarto, las decisiones de la Comisión que se dirigen a los Estados miembros, como es el caso del "Puerto Seguro", vincula a todos sus órganos[1094]. A partir de este principio, el Tribunal concluyó que las autoridades nacionales no pueden, en la evaluación de la idoneidad de un sistema fuera de la UE, incluso cuando están convencidos de la insuficiencia de la misma, «(…) *adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciara con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado* (…)»[1095]. Corresponde a la Comisión Europea adoptar la Decisión que compruebe que un tercer país garantiza un nivel de protección adecuado pero tal Decisión «*No obstante, una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos* (...)»[1096]. En otras palabras, las autoridades nacionales tienen la obligación y no la facultad de realizar una supervisión y control sobre las operaciones de transmisión de datos de un Estado miembro a un tercer Estado. La Decisión en cuestión no puede y no debe en modo alguno desviarse de lo que está contenido en la Directiva 95/46/CE en este sentido. Las autoridades competentes también deben ser capaces de realizar este trabajo teniendo en

[1093] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 40. El considerando 60 de la Directiva 95/46/CE establecía que las transferencias internacionales de datos hacia terceros Países «*sólo podrán efectuarse*» si, siguiendo sus artículos 25 y 26, los Países terceros garantizan «*un nivel de protección adecuado*». En caso contrario, deberá prohibirse la transferencia. Artemi RALLO LOMBARTE (2017: 607).

[1094] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 51. En particular, se especifica que: «(…) *las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ* (…)», publicados por el gobierno de EE.UU. que cumplen los principios de "Puerto Seguro" para la protección de la vida privada «(…) *con objeto de proteger los datos personales transferidos de un Estado miembro a Estados Unidos de América* (…)». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 7 y 6. Alicia CHICHARRO LÁZARO (2015: 1870-1871).

[1095] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 52. El principio de la supremacía del Derecho común sobre el Derecho interno, es decir, que las autoridades nacionales podrán adoptar actos contrarios a los de la Comisión Europea. En efecto, «*los actos de las instituciones de la Unión disfrutan en principio de una presunción de legalidad, y producen por tanto efectos jurídicos mientras no hayan sido revocados, anulados en virtud de un recurso de anulación*» (artículo 263 del TFUE) o «*declarados inválidos a raíz de una cuestión prejudicial*» (artículo 267 del TFUE) o «*de una excepción de ilegalidad*» (artículo 277 del TFUE). *Cfr*. sentencia del TJUE, *Comisión de las Comunidades Europeas contra República Helénica*, asunto C-475/01, sentencia de 5 de octubre de 2004, apartado 18.

[1096] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 53.

cuenta las condiciones de plena independencia, también a causa de la protección de los derechos consagrados en la CDFUE, en los artículos 7 y 8, y en virtud del artículo 25, apartado 6, de la Directiva 95/46, incumbe a esa autoridad «*examinar la referida solicitud con toda la diligencia exigible*»[1097].

150. Por esta razón, se reitera en conclusión sobre la primera cuestión planteada que «(…) *el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado*»[1098].

151. Como se ha indicado, la sentencia traza claramente una línea de atribución de competencias a las autoridades nacionales, que garantiza la protección de los derechos individuales. De hecho, el TJUE asigna a ellas directamente la evaluación de las solicitudes presentadas por los ciudadanos europeos, en lo que respecta a las garantías para la transferencia de datos[1099]. Y, por otro lado, sin embargo, se tiene en cuenta que, si bien las autoridades nacionales deben actuar con total independencia, esto no significa que puedan

[1097] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 63. Pero si la referida autoridad llegua a la conclusión de que «*los datos alegados en apoyo de esa solicitud son infundados y la desestime por ello, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión lesiva para ella ante los tribunales nacionales, esos tribunales están obligados a suspender el procedimiento y plantear al Tribunal de Justicia una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o, en su caso, suscitados de oficio son fundados*». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 64. La situación es diferente, sin embargo, en el caso contrario, es decir, cuando la autoridad nacional, llamada a evaluar la adecuación del sistema extra-UE sobre protección de datos por la persona que le haya presentado una solicitud, tenga en cuenta este sistema inadecuado y por lo tanto llega a conclusiones opuestas a las de la Comisión, la referida autoridad debe tener capacidad para comparecer en juicio. A ese efecto, corresponde al legislador nacional «*prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta*». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 65.

[1098] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 66.

[1099] La Decisión "Puerto Seguro", impide a las autoridades nacionales de control evaluar los reclamos de las personas que los necesiten para evaluar si la Decisión es compatible con la protección de la privacidad y los derechos fundamentales y las libertades de los individuos. En este contexto el Tribunal declara que la Comisión no era competente para reducir de este modo tales poderes en manos de las autoridades nacionales de supervisión y control.

eludir a las decisiones de la Comisión. Por esta razón, el juez europeo llegó a afirmar uno de los ejes centrales de la entera sentencia, o bien que el mismo juez «(…) *es exclusivamente competente para declarar la invalidez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, competencia exclusiva cuyo objeto es garantizar la seguridad jurídica preservando la aplicación uniforme del Derecho de la Unión*»[1100].

3.4. Acusación y desmantelamiento por el TJUE del sistema estadounidense de protección de datos. La anulación de la Decisión "Puerto Seguro"

152. Una vez superada esta cuestión, el TJUE va a la raíz del problema: la verificación de la adecuación efectiva de la protección prevista en los EE.UU.[1101]. Aunque la cuestión prejudicial planteada por el Tribunal Supremo de Irlanda fue dirigida sólo para obtener la interpretación de determinadas disposiciones de la Directiva 95/46/CE, los jueces de Luxemburgo, invocando la necesidad de dar una respuesta completa al tribunal nacional, optaron, no obstante, por ir más allá del *petitum*, asegurando también la validez de la Decisión "Puerto Seguro". Por lo tanto, el TJUE evaluó el alcance de la Decisión y del debilitado sistema norteamericano de protección de datos personales partiendo de que la adhesión de una entidad a los principios de "Puerto Seguro", siguiendo un sistema de autocertificación, requiere del «*establecimiento de mecanismos eficaces de detección y de control* (…) *para identificar y sancionar las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales*»[1102].

153. La importancia del tema se plantea de nuevo desde la diversidad de enfoque en el equilibrio de los intereses en conflicto que involucran la privacidad y protección de datos personales. Las inquietudes del demandante en el litigio principal, de hecho, fue sobre todo la actitud de EE.UU. con respecto al uso de los datos a los efectos de tutela del orden público y prevención del terrorismo.

154. Cabe señalar que la Directiva 95/46/CE no contenía una definición de "nivel de protección adecuado"[1103]. El TJUE parte de que la Directiva 95/46/CE no obligaba a los

[1100] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 61.
[1101] Ricard MARTÍNEZ (2015).
[1102] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 81.
[1103] En particular, el artículo 25, apartado 2, de la Directiva se limitaba a enunciar que: «(…) *el carácter adecuado del nivel de protección que ofrece un tercer país «se evaluará atendiendo a todas las circunstancias*

terceros Estados un nivel idéntico a aquel previsto de la norma, sino «(…) *exige que un tercer país «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales* (…)». Debe ser, por tanto, una protección «*sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46*», por lo que las garantías previstas por la Directiva no puedan eludirse mediante el recurso a la transferencia de datos fuera de la Unión Europea[1104]. La tarea de la Comisión, por tanto, es analizar si es posible establecer un nivel «*adecuado*» (artículo 25, apartado 6, de la Directiva 95/46/CE) de protección de las disposiciones de la legislación nacional y los compromisos asumidos a nivel internacional por el tercer país. El Tribunal afirma, que la Comisión tiene un margen de discreción reducida, poniendo en cuestión el derecho a la vida privada de un gran número de partes interesadas[1105].

155. En este sentido, los jueces de Luxemburgo ya se habían pronunicado fijando los principios presentes en la sentencia *Digital Rights Ireland*, que había dado lugar a la anulación de la Directiva 2006/24/CE. Esto es un indicio importante de la dirección en la que el razonamiento del Tribunal parece querer dirigirse.

156. A la luz de estas observaciones, el TJUE, sobre las disposiciones fundamentales de la Decisión "Puerto Seguro", lleva a cabo un desmantelamiento de los pilares para la transferencia de datos desde Europa a EE.UU., examinando si la Decisión puede ser considerada inválida. Es decir, el TJUE revisa la Decisión desde un punto de vista de su "constitucionalidad"[1106].

157. En primer lugar, el Tribunal se centra en el artículo 1 de la Decisión, en el mecanismo que considera satisfechos los principios de "Puerto Seguro" y garantizado un nivel adecuado de protección, cuando las empresas autocertifican su adhesión a estos

que concurran en una transferencia o en una categoría de transferencias de datos», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación». TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 70.

[1104] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 71 y 73.

[1105] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 75 y 78.

[1106] *Vid*. Massimo RUBECHI (2016), «Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)», en *federalismi.it*, núm. 23, pág. 22. El fallo *Digital Rights Ireland*, como ya expresado, inaugura una nueva fase de revisión judicial de carácter constitucional del Tribunal sobre el derecho secundario en vigor de la aplicación de los derechos fundamentales. El Tribunal no sólo comprueba las disposiciones de la Directiva 2006/24/CE mediante el recurso a los principios de estrecha necesidad y proporcionalidad, sino que también indica los elementos correctivos que permitirían superar los obstáculos de legitimidad. De esta manera, desempeña el papel típico de un Tribunal Constitucional que dispone indicaciones para el legislador de la Unión. Sobre el carácter de constitucional del TJUE, *vid*. también la primera parte de este Capítulo de la tesis.

principios[1107]. Los jueces de la UE, por un lado, han interpretado el término "adecuado" del artículo 25 de la Directiva 95/46/CE como "sustancialmente equivalente" a las normas de la UE, y, por otro lado, han excluido que una transferencia sea "adecuada" cuando se permite el acceso generalizado a los datos de la UE por las autoridades de inteligencia de EE.UU.[1108] (ver *infra* apartado 98 de la misma sentencia). El Tribunal también señala que los principios de "Puerto Seguro" sólo son aplicables a las empresas estadounidenses que se adhieren a ellos, mientras que las autoridades públicas en los EE.UU. no están sujetos a un régimen de este tipo. También, segun el articulo 2 de la Decisión "Puerto Seguro", ésta «*se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios de puerto seguro y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46 sin contener no obstante las constataciones suficientes sobre las medidas*» con las que EE.UU. garantiza un nivel de protección adecuado[1109], en el sentido del artículo 25, apartado 6, de la Directiva[1110], en consideración de su legislación nacional o de sus compromisos internacionales, «*a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas*»[1111].

158. Por otra parte, el TJUE constató que la aplicabilidad de los principios de "Puerto Seguro" podrían resultar limitados por exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense, incluso cuando la legislación estadounidense estableciera una obligación contraria a aquellos[1112]. Así pues, la Decisión "Puerto Seguro" reconoce la primacía de las «*exigencias de seguridad nacional, interés público y cumplimiento de la ley*» de EE.UU. sobre los principios de "Puerto Seguro", con el resultado de que las organizaciones con sede en los EE.UU. son incluso obligadas, sin limitación, a dejar de aplicar esos principios que han aceptado si están en conflicto con las necesidades

[1107] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 79 y 80.
[1108] *Vid*. Serena CRESPI (2016), «La nuova proposta di decisione di adeguatezza della Commissione europea riguardo agli Usa: lo scudo UE/USA per la privacy», en *Eurojus Centro di Eccellenza Jean Monnet presso l'Università degli Studi di Milano*. Disponible en Internet: http://rivista.eurojus.it/la-nuova-proposta-di-decisione-di-adeguatezza-della-commissione-europea-riguardo-agli-usa-lo-scudo-ueusa-per-la-privacy/ [consulta: 21 de octubre de 2016].
[1109] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 82 y 83.
[1110] Alicia CHICHARRO LÁZARO (2015: 1874). Es más, el artículo 25, apartado 2, de la Directiva 95/46 se limita a enunciar que el carácter adecuado del nivel de protección que ofrece un tercer País «*se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos*», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación.
[1111] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 71. Gloria GONZÁLEZ FUSTER (2014a: 168).
[1112] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 84 y 85. También Artemi RALLO LOMBARTE (2017: 608).

públicas y se manifiesten, por tanto, incompatibles con ellas[1113]. Por lo tanto, la Decisión incurre en «*posibles injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse*» desde la Unión a EE.UU., fundamentadas en «*exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley*» de EE.UU. En este sentido, «*para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no de manera efectiva los efectos de tal injerencia*»[1114]. Incluso, las personas afectadas no tenían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, si fuera necesario, su rectificación o supresión[1115].

159. Esta reconstrucción parece corroborada, según el Tribunal, mediante dos comunicaciones de 27 de noviembre de 2013 de la Comisión al Parlamento Europeo y al Consejo: en los puntos 2 y 3, apartado 2, de la Comunicación COM (2013) 846 final[1116]; y en los puntos 7, apartado 1 y 2, y 8 de la Comunicación COM (2013) 847 final[1117]. A partir de estas comunicaciones se desprende que «*las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a EE.UU. y tratarlos de manera incompatible*» con los propósitos de la transferencia, por ejemplo, también mediante la realización de un tratamiento que excede de lo «*estrictamente necesario y proporcionado para la protección de la seguridad nacional*»[1118]. El sistema de "Puerto Seguro" se aplica a las entidades privadas, pero no a las autoridades públicas de EE.UU., cuyas «*posibles injerencias en los derechos fundamentales de las personas*» no encuentran límites específicos y definidos[1119]. Las «*exigencias de seguridad nacional, interés público y*

[1113] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 86.
[1114] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 88 y 87.
[1115] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 90.
[1116] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Restablecer la confianza en los flujos de datos entre la UE y EE.UU., COM/2013/0846 final, 27/11/2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52013DC0846 [consulta: 25 de octubre de 2016].
[1117] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE (2013).
[1118] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 90.
[1119] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 88. «*EE.UU. y la UE, sobre todo la Comisión, deberían haber aclarado el ámbito de aplicación de dicha excepción, a fin de evitar cualquier interpretación o aplicación que anulase en esencia el derecho fundamental a la intimidad y la protección de datos*». En todo caso, esa excepción nunca debería haberse utilizado en menoscabo de la protección garantizada por la CDFUE y el resto de la legislación europea en materia de protección de datos. RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI)). Disponible en Internet:

cumplimiento de la ley» permiten dichas injerencias. El Parlamento Europeo, considera que el «*acceso a gran escala*» de las agencias de inteligencia de EE.UU. a los datos personales de la UE tratados según el principio de "Puerto Seguro" «*no cumple los criterios de exención en materia de seguridad nacional*»[1120]. El hecho de que las agencias de inteligencia americanas hayan tenido acceso de forma generalizada a los datos personales de los ciudadanos europeos pone de manifiesto que la protección de los mismos no es la adecuada.

160. A partir de los principios ya desarrollados en la sentencia *Digital Rights Ireland*[1121], el TJUE, después de recordar que la seguridad nacional es un principio fundamental de la UE de acuerdo con el artículo 52 apartado 1 de la CDFUE[1122], señala que los casos en los que las autoridades públicas de los Estados miembros y terceros puedan acceder a los datos personales de la UE son aquellos en los que «(…) *una normativa de ésta que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos*», y se permitirá sólo cuando sea «*estrictamente necesario*»[1123].

161. Desde esta perspectiva, los jueces europeos asumen que la Comisión Europea estaba obligada[1124] a evaluar si los EE.UU. en realidad aseguran, de conformidad con su propia legislación nacional o en virtud de los compromisos asumidos en el ámbito internacional, "un nivel de protección de los derechos fundamentales esencialmente equivalente a la de la

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES [consulta: 29 de octubre de 2016].

[1120] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014. Dicha resolución marcó el final de una investigación de seis meses realizada por el Parlamento Europeo sobre la vigilancia electrónica masiva de los ciudadanos de la UE, tras las revelaciones de junio de 2013 sobre las actividades de espionaje por parte de los EE.UU. y algunos Estados miembros. En esta resolución, también el Parlamento pidió la suspensión de los principios de "Puerto Seguro" y del Programa de Seguimiento de la Financiación del Terrorismo». *Vid*. *infra*, el Informe del Parlamento Europeo sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior (2013/2188(INI)), 21.2.2014.

[1121] *Vid*. *supra* apartados 54 y 55 de la sentencia *Digital Rights Ireland Ltd*.

[1122] María Isabel GONZÁLEZ PASCUAL (2014: 955). Las injerencias en el derecho a la protección de datos de carácter personal son posibles siempre que, respetando el contenido esencial del derecho: se prevean en una norma; respondan a un interés general; sean necesarias y proporcionadas; y los requisitos deben aplicarse de manera especialmente rigurosa.

[1123] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 91 y 92.

[1124] Alicia CHICHARRO LÁZARO (2015: 1875-1876).

UE, de conformidad con la Directiva 95/46/CE y a la luz de los artículos 7 y 8 de la CDFUE"[1125].

162. El TJUE realiza esta evaluación criticando firmemente la realidad estadounidense, y confirmando que: «*no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización*». También, el Tribunal añadió que «*una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta*»[1126]. Por último, de igual manera «*una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta.* (…) *la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho*»[1127]. En fin, el TJUE, en la evaluación de la equivalencia de la protección prevista en el tercer país, reconoce la ausencia de un instrumento legislativo necesario para evitar poner en peligro el contenido esencial de los derechos en juego, y también de los mecanismos de protección judicial[1128].

[1125] Además, la Comisión en sus comunicaciones señaló que los interesados no tenían los recursos administrativos o legales, en particular, con el fin de permitir el acceso a los datos que les conciernan y, en su caso, para obtener la corrección o supresión. Y una normativa que no prevé posibilidad alguna de que el justiciable posea acciones legales para acceder a sus datos personales o para obtener su rectificación o supresión vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva. TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 90.

[1126] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartados 93 y 94. Véase, en ese sentido, la sentencia del TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 39.

[1127] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 95.

[1128] Ricard MARTÍNEZ (2015). El Tribunal concluye, sin embargo, que la Comisión «(…) *no manifestó en la Decisión 2000/520 que Estados Unidos «garantiza» efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales*», limitándose simplemente a examinar los conjuntos de principios de "Puerto Seguro". TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 97.

163. A partir de todos estos argumentos, el Tribunal considera que «*el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa*»[1129]. En definitiva, el TJUE dictamina que la Decisión es inválida y no ofrece ni asegura ninguna protección adecuada a los datos personales.

164. El Tribunal, de nuevo en una forma muy similar a la sentencia de *Digital Rights Ireland*[1130], procede a anular la Decisión "Puerto Seguro" con efecto retroactivo (*ex tunc*), como una ulterior toma de posición del Tribunal a favor del derecho a la vida privada. Es significativo que una vez más, esto ocurra en un hecho relativo al equilibrio entre las preocupaciones de seguridad, prevención y represión de la delincuencia, por un lado, y la protección del derecho fundamental a la vida privada, por otro. Esto es lo que ocurrió no sólo en *Digital Rights Ireland* sino también en el caso *Schrems*, donde, además de los perfiles económicos relacionados con grandes empresas de EE.UU., el núcleo del problema venía representado por las necesidades de investigación e inteligencia de las autoridades federales. Y en estas dos sentencias, el Tribunal utiliza una referencia de origen interpretativa para la evaluación de la validez de un acto de Derecho derivado, actuando como juez constitucional de facto.

165. En este sentido, se registra una cierta determinación reformadora del TJUE en relación con las fuentes de la UE, especialmente en la afirmación de la primacía otorgada a los derechos humanos, principalmente el derecho a la protección de datos personales. A partir de la sentencia *Schrems*, cesaron todas las transferencias de datos hacia EE.UU. al amparo del "*Safe Harbour*"[1131], haciéndose urgente negociar un nuevo marco jurídico para esta concreta dimensión de la relación transatlántica[1132].

[1129] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 98.
[1130] La propuesta de suspender la aplicación de la Directiva anulada sólo por el futuro, de hecho, fue avanzada en las conclusiones del Abogado General en el caso *Digital Rights Ireland*.
[1131] Debe aclararse que la anulación de la Decisión 520/2000/CE no implica que desaparezcan las transferencias de datos personales hacia los EE.UU., ya que puede llevarse a cabo sobre la base del consentimiento expreso o sobre la base de las reglas corporativas vinculantes (*Binding Corporate Rules - BCR*). Por lo que el interesado puede dar su consentimiento a la transferencia o el responsable del fichero podrá adoptar las normas de gestión aprobadas por las autoridades nacionales de protección que permitirán la transferencia. Cambia el hecho de que no se pudo seguir utilizando el sistema "Puerto Seguro", es decir trasladar los datos hacia los EE.UU. sin consentimiento o sin reglas ya aprobadas, es decir tanto los datos protegidos en los EE.UU. como en Europa, con mayores cargas de gestión para quien traslada los datos de Europa a los EE.UU. Para una mayor información sobre las reglas corporativas vinculantes, *vid*. el sitio web de la Comisión Europea, *Overview on Binding Corporate rules*: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm [consulta: 11 de noviembre de 2016].
[1132] Juan Fernando LÓPEZ AGUILAR (2017: 577).

3.5. El impacto de la sentencia del TJUE en las relaciones transatlánticas

166. El 6 de octubre de 2015, el TJUE dio a conocer la sentencia que se esperaba en el caso *Schrems vs. Facebook*[1133], anulando, después de 15 años, la Decisión 520/2000/CE de la Comisión Europea. La sentencia no entra a evaluar los principios de "Puerto Seguro", que atribuyó la idoneidad de las transferencias de datos personales producido bajo los principios, confirmando que: a) la legislación que «*permite a las autoridades públicas acceder*» de "manera generalizada" «*al contenido de las comunicaciones electrónicas*» debe considerarse comprometedora de la esencia del derecho fundamental al respeto de la vida privada[1134]; b) el régimen de "Puerto Seguro" permite la interferencia de las autoridades públicas de EE.UU. violando tres derechos fundamentales como el derecho a la protección de los datos personales, la confidencialidad de las comunicaciones en el contexto de la vida privada y familiar, y el «*derecho a la tutela judicial efectiva*», de conformidad con los artículos 7, 8 y 47 de la CDFUE[1135]; c) el contenido de la Decisión de la Comisión Europea no puede eliminar ni siquiera reducir las facultades de que disponen las autoridades nacionales de supervisión; d) las autoridades de protección de datos personales tienen competencia para evaluar la idoneidad de la legislación de privacidad con respecto a la Directiva Europea 95/46/CE en el país de destino de los datos personales (en este caso EE.UU.), y esta prerrogativa no puede verse limitada ni tampoco reducida por decisiones de

[1133] Las implicaciones de esta sentencia han sido foco de atención especial también por parte del Grupo de Trabajo que ha dedicado una sesión especial plenaria a ese asunto. Al término de la sesión, el Grupo adoptó una declaración en la que, además de dar las primeras indicaciones en aspectos relacionados con la transferencia de datos hacia EE.UU., también puso de manifiesto la necesidad de adoptar una posición común en la aplicación de la sentencia, señalando que la vigilancia masiva e indiscriminada, punto central de la decisión del Tribunal, es incompatible con el marco europeo, y reiteró la necesidad de que las instituciones europeas y los Estados miembros iniciaran un diálogo con EE.UU. para el logro de soluciones legales que garantizasen que la transferencia de datos en el extranjero cumple con los derechos fundamentales. Tras la anulación de la Decisión "Puerto Seguro", las cláusulas contractuales tipo y las *BCR* (reglas corporativas vinculantes) todavía pueden ser usadas. Sin embargo, las transferencias que se lleven a cabo bajo dicha Decisión son consideradas ilegales (es decir, sin base jurídica). De hecho, según lo declarado formalmente por el Grupo de Trabajo, la fecha oficial para encontrar una solución adecuada con las autoridades de los EE.UU., habría sido el 31 de enero de 2016, fecha en la que las autoridades de protección de datos de la UE se comprometen a tomar todas las medidas necesarias y apropiadas, que pueden incluir medidas de aplicación coordinadas de aplicación de la ley. Las autoridades de protección de datos tienen, de hecho, la facultad de suspender o prohibir, además de sancionar, las transferencias en los casos en los que las supuestas garantías no se consideren suficientes. Sus poderes se utilizarán siempre que sea posible de manera coordinada, especialmente si las instituciones de la UE y los Estados miembros no identifican una solución política que tenga en cuenta la necesidad de respetar el contenido esencial del derecho fundamental a la protección de datos incluidos en las transferencias de datos a terceros Países. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2015e), Statement of the Article 29 Working Party, Brussels, 16 October 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [consulta: 15 de noviembre de 2016]; y «Las Autoridades europeas de Protección de Datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el Puerto Seguro», en *AGPD*, Madrid, 19 de octubre de 2015.

[1134] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 94.

[1135] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 107, punto 1.

la Comisión[1136]; y que e) el TJUE es el único competente para declarar que un acto de la UE, tal y como es el caso de una Decisión de la Comisión, no es válido[1137].

167. Con esta sentencia, el Tribunal va mucho más allá de la cuestión planteada y anula en su totalidad la Decisión de la Comisión 2000/520/CE. En este aspecto, el Tribunal no sólo afecta al sistema de transferencia de datos que había encontrado en la Decisión anulada su base de legitimidad, sino que afecta a los fundamentos mismos de todo el sistema de tratamiento de datos por las grandes empresas de la Web[1138]. Además de cuestionarse la protección de los datos personales por parte de los operadores de las redes sociales, y en concreto la legalidad de las *privacy policy* por *Facebook*[1139], la cuestión esencial sobre la que se desarrolla la evaluación del Tribunal es el sistema de vigilancia masivo creado por los EE.UU. en el que los grandes gestores de servicios de Internet se han visto implicados. La evaluación del Tribunal europeo, por lo tanto, pone en duda su compatibilidad con el sistema de protección de datos personales en Europa y con ello suscita la problemática

[1136] A este respecto, resulta interesante cómo la sentencia contribuye a la articulación de competencias entre las autoridades públicas, nacionales y europeas, en el contexto de la aplicación de las disposiciones contenidas en la Directiva de 1995. De hecho, al excluir el monopolio exclusivo de la Comisión Europea para evaluar la adecuación del nivel de protección de datos ofrecido por el tercer país y al reconocer, por el contrario, que existe una discrecionalidad significativa en las autoridades de supervisión, el TJUE exige que dicha evaluación sea realmente objetiva a fin de ofrecer una protección eficaz a las personas cuyos datos se transfieren de la UE a un Estado no miembro (no sólo sustantivamente, sino también a nivel de procedimiento). Esta es, en particular, la obligación impuesta a estas autoridades para llevar a cabo sus funciones, que se hagan de una manera objetiva e imparcial, sustrayéndose a cualquier tipo de influencia externa, a partir de la influencia directa o indirecta del Estado miembro. La garantía de independencia de las autoridades de supervisión es un elemento importante de la estructura de la Directiva 95/46/CE, teniendo en cuenta las conclusiones del TJUE en relación con la incapacidad de la Comisión, en virtud del artículo 25, apartado 6, para limitar los poderes de las autoridades. La novedad de esta sentencia no reside tanto en la enunciación de las competencias conferidas a las autoridades de control de los datos (poderes de investigación y de intervención), sino también en su extensión a los casos de transferencias de datos de la UE a países terceros. De este modo, los jueces demuestran una particular sensibilidad con respecto a la protección de la intimidad de las personas implicadas y, por lo tanto, una voluntad firme de reconocer una protección equivalente a los datos personales ya se procesen en Europa o se transfieran a un Estado tercero. Michele NINO (2015).

[1137] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 61.

[1138] Al margen de lo positivo de este planteamiento, la decisión de no limitar los efectos de la sentencia había provacado un *gap* legislativo que conllevaba el riesgo de repercusiones económicas graves debido al elevado número de relaciones jurídicas constituidas de buena fe, y en presencia de inseguridad jurídica objetiva y significativa. La ausencia de un nuevo Acuerdo de "Puerto Seguro", por supuesto había creado una incertidumbre regulatoria sobre la transferencia de datos a todas las empresas que necesitan para mover datos personales entre la UE y EE.UU., lo que afectaba a más de 5.500 empresas, entre ellas muchos nombres bien conocidos de Internet como Google, Facebook, Apple, Microsoft, Yahoo!, *etc*. El bloque de transferencia de los datos más allá de las fronteras de Europa no sólo obligaba a las empresas a adoptar normas más complejas y costosas, sino también a cambiar la forma en que obtienen beneficios en Europa. Las transferencias de datos resultan vitales para el desarrollo de las empresas y, por eso, el logro del éxito de las negociaciones es fundamental. De otro modo, se impondrían obstáculos al normal desenvolvimiento de las empresas y supondría dar marcha atrás o rechazar un Acuerdo que, aunque con sus más y sus menos y con aspectos mejorables, era un marco eficaz, que proporcionaba seguridad jurídica y había venido funcionando durante años.

[1139] Según algunos expertos, serán más fáciles abrir investigaciones por parte de las autoridades nacionales sobre empresas como *Facebook* por presuntas violaciones a la normativa sobre privacidad. Mark SCOTT (2015a), «Data Transfer Pact Between U.S. and Europe Is Ruled Invalid», en *The New York Times*, oct. 6.

cuestión del tratamiento de los datos personales fuera de la UE que requiere grandes precauciones.

168. El pronunciamiento da lugar a una dura crítica de los sistemas de protección de datos personales y privacidad ofrecidos tanto por el sistema "*Safe Harbor*"[1140] como por el ordenamiento jurídico de los EE.UU. en su conjunto, a través de una comparación entre el mismo y los principios europeos en materia. Esta crítica parece fundarse en el hecho de que, a diferencia de las normas de la UE en las que, desde la entrada en vigor del Tratado de Lisboa, los derechos a la privacidad y la protección de datos son considerados fundamentales y disciplinados en detalle[1141], el sistema jurídico estadounidense no realiza ese reconocimiento y no prevé una legislación precisa y uniforme para proteger adecuadamente esos derechos, sino una legislación fragmentaria y sectorial que hace que sea extremadamente insegura y peligrosa la circulación de los datos[1142]. El TJUE pone el fin del Acuerdo ante las repetidas y probadas ineficiencias, por los estadounidenses, en la efectiva protección de los datos de las personas en el territorio de EE.UU.

169. Se comprueba así que esta sentencia forma parte de la tendencia más amplia de la UE, que considera que el ordenamiento jurídico de los EE.UU. es inadecuado a la salvaguardia del derecho a la privacidad individual. De hecho, los numerosos acuerdos entre la UE y EE.UU., que regulan tanto la transferencia de datos *PNR* como la transmisión de datos bancarios y financieros entre ambos lados del Atlántico, han sido desde siempre fuertemente criticados porque se consideran incapaces de garantizar el cumplimiento de los principios de la UE sobre protección de datos personales. Los efectos de la sentencia, ya en este punto claramente extendida, alcanzan también a terceros países que han firmado

[1140] La totalidad de empresas estadounidenses involucradas en el programa "*PRISM*", que permitió a las autoridades estadounidenses durante un largo tiempo acceso ilimitado a los datos de telecomunicaciones almacenados y procesados en los EE.UU., habían autocertificado sus adhesiones a los principios de "Puerto Seguro". *Vid*. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE (2013).

[1141] Fuera de la UE no existe, en la actualidad, un sistema similar de protección de datos personales, tales como el vigente en Europa, que reconozca la protección de datos como derecho fundamental del individuo. La mencionada decisión del Tribunal representa un paso más hacia el establecimiento de una "soberanía digital de la Unión Europea". Soberanía, entendida ésta en su sentido tradicional, o bien como «*il potere di controllare, de iure e de facto, un certo spazio, le attività che ivi si svolgono, coloro che vi entrano, come tale spazio è organizzato, amministrare poteri di polizia, giudiziari e di sicurezza in tale spazio*». *Cfr*. Giorgio RESTA, Vincenzo ZENO-ZENCOVICH (2016: 7).

[1142] Este punto de vista está en total contradicción con los grandes flujos de datos intercambiados entre la UE y los EE.UU. en todo momento y en todos los niveles, que es la base del equilibrio global actual en el comercio, social y política.

acuerdos con la UE en el ámbito de la transferencia de datos[1143], y también podría tener un impacto en terceros países que han adoptado el modelo de la UE para la adopción de los respectivos acuerdos (por ejemplo, el caso de Suiza).

170. La línea jurisprudencial del TJUE sigue, sobre todo en los últimos años, un curso lineal y consecuente, articulado en torno a un criterio de máxima protección de la privacidad y los datos personales, como alternativa a las deficiencias surgidas en este ámbito a partir de la adopción de la Directiva de 1995. Los jueces se convierten en guardianes de la protección de la privacidad y de los datos personales en Europa (de conformidad con la sentencia *Digital Rights Ireland* de 2014, en la que declaró la invalidez del sistema de retención de datos indiscriminado y duradero), declaran en última instancia la necesidad de que la transferencia de información personal entre UE y EE.UU. sea enfocada a la observancia efectiva de los principios de la legislación europea, primaria y secundaria.

171. Esta reacción del TJUE obedece a determinadas actividades de vigilancia masiva e indiscriminada realizadas en los últimos años que afectan de forma directa a cada individuo, que ve comprometida la confidencialidad de sus datos. Sin embargo, los últimos ataques terroristas han demostrado que la vigilancia masiva no ha ayudado a evitarlos. Existe un mayor riesgo de uso alterado y generalizado de la información, mientras que lo que se necesita –y que el Tribunal ha declarado repetidamente, incluso en los casos mencionados anteriormente– es una actividad de control contemplada y concreta, no disuelta y, por eso, inútil.

172. También parece evidente la intención del Tribunal de reforzar su posición en el papel de suplencia política[1144] a expensas de las instituciones políticas europeas. Por medio de las

[1143] Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes: Suiza (Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000); Canadá (Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos); Argentina (Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003); Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003); Isla de Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004); Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008); Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010); Andorra (Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010); Israel (Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011); Uruguay (Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012); Nueva Zelanda (Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012). *Vid*. «Transferencias internacionales de datos», en *AGPD*. Disponible en Internet: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consulta: 03 de diciembre de 2016].

[1144] Giusella FINOCCHIARO (2016), «La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems», en Giorgio RESTA, Vincenzo ZENO-ZENCOVICH, *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, RomaTrE-Press,

sentencias mencionadas, el Tribunal define los límites de los poderes soberanos, gobernando con absoluta claridad, a través de la supremacía judicial[1145], sobre los temas más sensibles como la protección de datos y política internacional. Por lo tanto, tal y como sucedió con las sentencias anteriores del Tribunal, se suele considerar que éstas tienen eficacia relevante sólo en Europa[1146], lo que resulta erróneo, ya que las repercusiones y reacciones van mucho más allá de las fronteras europeas. Las sentencias en cuestión tienen una consecuencia extraeuropea, porque en ellas se afectan cuestiones que no se someten a los límites en los que tradicionalmente operan los tribunales, lo que conduce a un discurso de regulación política entre ambos lados del Atlántico[1147].

---

págs. 116 y ss. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/PTD [consulta: 17 de diciembre de 2016].

[1145] Sobre el activismo judicial y la debilidad de la clase política, resulta interesante el estudio de STAIANO. El autor enfatiza que ese activismo judicial se produjo y obtuvo consenso debido a la falta de decisiones políticas. Y si, en este caso, la orientación del TJUE está en *bonam partem*, para proporcionar una mayor garantía de derechos, aunque no siempre puede ser así, como lo demuestran las oscilaciones en materia de protección de la privacidad. Sin embargo, las "políticas jurisprudenciales" se superponen y prevalecen sobre las políticas legislativas, incluso en la implementación constitucional, y la valoración de la reconciliación de los valores y los derechos en juego se resta de la representación política que se confiarán al equilibrio judicial. En Sandro STAIANO (2017: 16 y ss.).

[1146] Siguiendo la línea de la importancia política de las consecuencias, al día siguiente de la sentencia, los gobiernos europeos estaban divididos sobre la cuestión. Francia y Alemania han defendido la necesidad de aumentar la protección de los datos de sus ciudadanos. Otros países, como el Reino Unido e Irlanda (donde muchas empresas de Silicon Valley tienen su sede europea), han defendido el lugar del "Puerto Seguro". En relación con la decisión del TJUE en el caso *Schrems*, las autoridades de protección de datos de Alemania publicaron una declaración conjunta sobre las transferencias de datos personales de la UE hacia los EE.UU. en general y en particular sobre el "*Safe Harbor*". Además de poner de relieve la independencia de las autoridades de protección de datos y abandonar con efecto inmediato el "*Safe Harbor*" como mecanismo válido para las transferencias de datos a EE.UU., la declaración se centra incluso sobre las normas corporativas vinculantes, las cláusulas contractuales estándar y el consentimiento de la persona interesada. Las autoridades de protección de datos alemanes afirman que no concederán nuevas autorizaciones para el uso de instrumentos alternativos. Vid. «Safe-Harbor - Update (26.10.2015)», Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder. Disponible en Internet: https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.html [consulta: 12 de diciembre de 2016].

[1147] Las señales de una verdadera voluntad política para mejorar las relaciones entre la UE y los EE.UU., parecen encontrarse en enero de 2014, cuando el presidente estadounidense Barack Obama confirmó la necesidad de reformar algunos aspectos en materia de inteligencia y vigilancia masiva. En este sentido, Obama presentó la *Presidential Policy Directive* (*PPD-28*), que establece una serie de principios generales que rigen y restringen la recopilación masiva de datos y que tiene por finalidad la seguridad nacional, comprometiéndose a establecer claras limitaciones en lo relativo a la recopilación masiva de datos, asegurando garantías y mecanismos de supervisión de las actividades de inteligencia. En esta línea, el 20 de octubre de 2015, la Cámara de Representantes de los EE.UU. (*US House of Representatives*) acordó avanzar la *Judicial Redress Act* (*JRA*) (Ley de Recurso Judicial), que garantizaría a algunos extranjeros el derecho a ejercer sus derechos de privacidad en los tribunales estadounidenses. La aprobación de la *JRA* fue firmada por el presidente Obama el 24 de febrero de 2016, la cual abre las puertas de los tribunales de EE.UU. a los ciudadanos europeos para quejas sobre el uso de los datos. La *JRA* autoriza al Departamento de Justicia de EE.UU. a designar a países extranjeros u organizaciones regionales de integración económica cuyos ciudadanos naturales puedan entablar acciones civiles en virtud de la Ley de Privacidad de 1974 (*Privacy Act of 1974*) contra ciertas agencias del gobierno de los EE.UU. con el propósito de acceder, enmendar o corregir las revelaciones ilegales de los registros mantenidos por una agencia. *Vid*. «US on its way to adopt Judicial Redress Act and hopefully facilitate transfers from the EU», en *Privacy Laws & Business*, 21/10/2015; y H.R.1428 - Judicial Redress Act of 2015, Public Law N.: 114-126 (02/24/2016). Disponible en Internet: https://www.congress.gov/bill/114th-congress/house-bill/1428 [consulta: 12 de diciembre de 2016].

173. La decisión del TJUE llegó en un contexto de fuerte tensión transatlántica y la presión política a la Comisión por parte del Parlamento Europeo y también del gobierno de EE.UU., fue muy intensa, adelantando, *de facto*, la sustitución de la Directiva de 1995 en tanto se estaba negociando la aprobación del RGPD. A la luz, por lo tanto, del contexto general en el que se dictó la sentencia *Schrems*, puede llegarse a la conclusión de que la elección del Tribunal de Luxemburgo, de intervenir tal y como lo hizo sobre el Acuerdo de "Puerto Seguro", se debe a razones de política en sentido estricto. En consecuencia, debe tenerse en cuenta que todas las sentencias anteriores, aunque dictadas conforme al contenido de la Directiva de protección de datos, describen un marco de herramientas de protección que tienen mayor relación con el nuevo RGPD.

174. Esta importante sentencia, implicó, como se ha indicado, no sólo una aceleración potencial de la reforma de la legislación europea en materia de protección de datos, sino también renegociar las condiciones en materia de privacidad y seguridad de datos que debían regir en las transferencias internacionales UE-EE.UU.[1148], con el fin de neutralizar cualquier posible riesgo que aquellas pudieran suponer para la protección de la vida privada, los derechos y las libertades fundamentales de los titulares de los datos personales.

175. A tal fin, después de varios meses de negociaciones la Comisión Europea y el gobierno de EE.UU. llegaron finalmente a un Acuerdo sobre la transferencia a los EE.UU. de información personal recogida en la UE. Las negociaciones, iniciadas en realidad desde las revelaciones "*Datagate*"[1149], se habían acelarado de forma sustancial después de la intervención del TJUE con la sentencia *Schrems* de 2015[1150], y tenían como objetivo definir

[1148] Para un análisis detallado de los acuerdos de transferencia de datos entre la UE y los EE.UU., *vid*. Francesca BIGNAMI (2007b), «European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining», en *Boston College Law Review*, vol. 48, págs. 609-698. Disponible en Internet: http://scholarship.law.gwu.edu/faculty_publications/225/ [consulta: 17 de diciembre de 2016]; Paul M. SCHWARTZ (2013), «The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures», en *Harvard Law Review*, vol. 126, págs. 1966-2009. Disponible en Internet: https://harvardlawreview.org/2013/05/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/ [consulta: 17 de diciembre de 2016]; y, sobre todo, Cristina BLASI CASAGRAN (2016b), *Global Data Protection in the Field of Law Enforcement: An EU perspective*, London; N.Y., Routledge, págs. 264.

[1149] La Comisión Europea y los EE.UU., han estado durante mucho tiempo involucrados en el tema de las transferencias de datos en el contexto del proceso de revisión del "Puerto Seguro" que se inició en noviembre de 2013. *Vid*. respectivamente, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Restablecer la confianza en los flujos de datos entre la UE y EE.UU. (2013) y COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE (2013).

[1150] El 6 de noviembre de 2015, la Comisión Europea se apresuró a publicar directrices sobre la transferencia de datos personales de los ciudadanos europeos en los EE.UU. e instó a que se estableciera rápidamente un nuevo marco tras la sentencia *Schrems*. En su Comunicación, la Comisión subraya los puntos siguientes: «*el régimen de puerto seguro ya no constituye una base jurídica para la transmisión de datos personales a los*

un nuevo Acuerdo Marco de Protección de Datos entre la UE y los EE.UU. y la necesidad de crear un nuevo texto que sustituyera al Acuerdo de "Puerto Seguro" anulado por el TJUE: el llamado "Escudo de la privacidad UE-EE.UU." (en adelante, "Escudo de la privacidad"). Estos dos instrumentos jurídicos mantienen una estrecha relación en cuanto a su contenido. Mientras que el Acuerdo Marco regula las transferencias de datos entre entes gubernamentales de los EE.UU. y la UE, el "Escudo de privacidad" fija normas para los flujos de datos transferidos entre los EE.UU. y la UE por parte de compañías privadas con fines puramente comerciales. Aunque puede parecer a primera vista que existe una separación clara entre estas dos áreas, la estrecha cooperación entre entes públicos y privados en el intercambio de datos personales hace imprescindible que ambos Acuerdos internacionales mantengan una coherencia entre sí, y también con las normas de protección de datos de la UE[1151] (*amplius infra*).

176. Por fin, el 2 de febrero de 2016, la Comisión puso a disposición la documentación relativa a un nuevo sistema, que sustituye el "Puerto Seguro", llamado "Escudo de la privacidad UE-EE.UU." (en inglés, "*EU-U.S. Privacy Shield*")[1152] para permitir la libre transferencia de datos personales a las empresas estadounidenses que se adherirán[1153] (vid.

Estados Unidos; la Comisión proseguirá y concluirá las negociaciones de un nuevo y sólido marco para las transferencias transatlánticas de datos personales, que debe cumplir los requisitos identificados en la sentencia del Tribunal, en particular por lo que se refiere a las limitaciones y garantías del acceso a los datos personales por parte de las autoridades públicas de los Estados Unidos; deberán modificarse otras decisiones de adecuación a fin de garantizar que las autoridades de protección de datos (APD) sigan teniendo libertad para investigar las quejas presentadas por particulares». COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems), COM(2015) 566 final, Bruselas, 6.11.2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52015DC0566 [consulta: 23 de diciembre de 2016]; y COMISIÓN EUROPEA - Comunicado de prensa (2015b), La Comisión publica orientaciones sobre las transferencias transatlánticas de datos e insta al rápido establecimiento de un marco renovado tras la sentencia en el asunto Schrems, Bruselas, 6 de noviembre de 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-6015_es.htm [consulta: 23 de diciembre de 2016].

[1151] Cristina BLASI CASAGRAN (2017), «Nuevo Régimen Jurídico para la Transferencia de Datos entre la UE y los Estados Unidos ¿Es compatible con la Normativa Europea de Protección de Datos?», en *Revista General de Derecho Europeo*, núm. 42, pág. 194. Disponible en Internet: https://www.researchgate.net/publication/317662622 [consulta: 07 de septiembre de 2017].

[1152] Se enumeran a continuación algunos artículos de los principales periódicos británicos y estadounidenses sobre la noticia del nuevo Acuerdo "*Privacy Shield*", en los que se resaltan los puntos fuertes del Acuerdo, las críticas y los obstáculos para hacerlo ejecutivo en todos los aspectos: E.L. (2016), «The new transatlantic data "Privacy Shield», en *The Economist*, feb 2nd. Disponible en Internet: http://www.economist.com/blogs/economist-explains/2016/02/economist-explains-2; Mark SCOTT (2016), «U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await», en *The New York Times*, feb. 2; Samuel GIBBS and Owen BOWCOTT (2016), «'Robust' deal reached to preserve privacy of EU-US data sharing», en *The Guardian*, tuesday 2 february. Disponible en Internet: http://www.theguardian.com/technology/2016/feb/02/robust-deal-reached-to-preserve-privacy-of-eu-us-data-sharing [artículos consultados: 07 de septiembre de 2017].

[1153] COMISIÓN EUROPEA - Comunicado de prensa (2016a), La Comisión Europea y los Estados Unidos acuerdan un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad UE - EE.UU., Estrasburgo, 2 de febrero de 2016. Disponible en Internet: http://europa.eu/rapid/press-release_IP-16-

infra). El nuevo Acuerdo político[1154] obliga a las empresas que operan en los EE.UU. a proteger mejor los datos personales de los ciudadanos europeos y refuerza los poderes de control y ejecución del Departamento de Comercio de EE.UU. y la Comisión Federal de Comercio de EE.UU., gracias a una mayor cooperación con las autoridades europeas de privacidad. En el mismo, se fija el compromiso de EE.UU. de garantizar que las autoridades públicas tienen acceso, por ley, a los datos personales transferidos bajo el nuevo régimen bajo condiciones y limitaciones claras, y como parte de un sistema de vigilancia, impidiendo así el acceso generalizado[1155].

216_es.htm [consulta: 26 de febrero de 2016]; Statement From U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield, February 2, 2016. Disponible en Internet: https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield [consulta: 26 de febrero de 2016].

[1154] El Grupo de Trabajo acogió con satisfacción la conclusión de las negociaciones entre la UE y los EE.UU. sobre la introducción de un "Escudo de la privacidad UE-EE.UU.", dentro del plazo fijado por el Grupo mismo en su Declaración de 16 de octubre de 2015. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2015e). Del mismo modo expresó algunas dudas acerca este Acuerdo, ya que actualmente carecía de un texto oficial para conocer con precisión el contenido y la vinculación jurídica del Acuerdo, por lo que no existen elementos que indiquen que el "*Privacy Shield*" proporciona un nivel de protección adecuado y responde a las preocupaciones más amplias planteadas por la sentencia *Schrems* en lo que respecta a las transferencias internacionales de datos personales. En particular, la jurisprudencia europea sobre los derechos fundamentales establece cuatro garantías esenciales para las actividades de inteligencia: el procesamiento debe basarse en normas claras, precisas y accesibles, lo que significa que cualquier persona que esté razonablemente informada debe ser capaz de prever lo que podría suceder con sus datos cuando los transfiera; es necesario demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos perseguidos, para lo que es necesario encontrar un equilibrio entre el objetivo para el que se recopilan y se accede a los datos (generalmente la seguridad nacional) y los derechos del individuo; debe existir un mecanismo de supervisión independiente, que sea eficaz e imparcial, puede ser un juez u otro órgano independiente, siempre y cuando tenga capacidad suficiente para realizar los controles necesarios; los recursos efectivos deben estar a disposición del individuo, cualquier persona debe tener el derecho de defender sus derechos ante un organismo independiente. ARTICLE 29 DATA PROTECTION WORKING PARTY (2016a), Statement of the Article 29 Working Party on the consequences of the Schrems judgment, Brussels, 3 February 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf [consulta: 26 de febrero de 2016].

[1155] El nuevo mecanismo incluía los siguientes elementos: a) Obligaciones rigurosas para las empresas que trabajan con los datos personales de los europeos y estricta aplicación: las empresas estadounidenses que quieran transferir los datos procedentes de Europa tienen que asumir obligaciones específicas en relación con el procesamiento de datos y el respeto de los derechos de las personas involucradas. La Comisión Federal de Comercio de EE.UU. se encargará de supervisar el cumplimiento de estas obligaciones. Por otra parte, en algunos casos, las empresas en cuestión se comprometerían a actuar de acuerdo con las decisiones de las autoridades de protección de datos europeas. b) Salvaguardias y «*obligaciones en materia de transparencia claras para el acceso de la administración estadounidense*»: los EE.UU. aseguran la existencia de límites claros a la posibilidad de que las autoridades de inteligencia tengan acceso a datos personales: no habrá actividades de vigilancia indiscriminada y no proporcional. c) Protección eficaz de los derechos de los ciudadanos de la UE con varias posibilidades de recurso: los ciudadanos europeos que consideren que sus derechos son violados en los EE.UU. tendrán diferentes medios de protección: la posibilidad de que las autoridades europeas de protección de datos lleven los casos a la Comisión Federal de Comercio de EE.UU., o ponerse en contacto con un Ombudsperson creado específicamente para violaciones de las autoridades de la inteligencia. *Vid*. COMISIÓN EUROPEA - Comunicado de prensa (2016a).

3.5.1. Las transferencias internacionales de datos personales y el reto de salvaguardar los derechos fundamentales en el "Escudo de la privacidad UE-EE.UU." ("EU-US Privacy Shield"). ¿Más protección contra la injerencia de EE.UU.?

177. La Decisión "Escudo de la privacidad" resulta especialmente importante porque sirve de puente para salvar la anulación de la anterior Decisión "Puerto Seguro" por el TJUE mediante la sentencia *Schrems vs. Facebook* que impedía a las empresas transferir datos desde la UE a los EE.UU. en condiciones seguras desde la perspectiva de protección de datos. La imposibilidad de contar con un sistema de cobertura para la transferencia de datos que se había venido utilizando durante quince años por muchas empresas creó una comprensible preocupación en la industria, por lo que era necesaria una intervención urgente por parte de la Comisión Europea[1156].

178. Al margen de estos logros, lo que importa aquí es proporcionar una breve descripción y una primera evaluación de las nuevas normas contenidas en el "Escudo de la privacidad", con especial atención a las excepciones a las normas sobre protección de datos personales justificadas por razones relacionadas con la seguridad nacional y las dudas de su compatibilidad con la normativa de la UE, especialmente con respecto a un posible futuro pronunciamiento del TJUE.

179. Resulta interesante analizar la elección del nombre de esta Decisión para aclarar algunas cuestiones que se van a analizar a continuación. Como se ha señalado de forma

[1156] A partir de las decisiones de adecuación de la Comisión Europea, los datos personales de la UE pueden ser transferidos a terceros Estados simplemente siguiendo las reglas contenidas en dichas decisiones. Por lo tanto, las decisiones de adecuación son entonces las mejores herramientas para las empresas, ya que resultan más completas, simples y, por lo tanto, menos costosas para llevar a cabo las transferencias de datos personales entre la UE y terceros Estados. Debe tenerse en cuenta que, en ausencia de una decisión de adecuación que se establezca para todos los Estados miembros las condiciones bajo las cuales los datos personales de la UE pueden ser transferidos a terceros países, resulta difícil lograr un nivel similar de seguridad jurídica mediante las alternativas previstas en el artículo 26 de la Directiva 95/46/CE, a saber, las cláusulas contractuales y normas corporativas vinculantes. En tales casos, la responsabilidad de garantizar un nivel adecuado de protección en virtud del artículo 25 de la Directiva en el contexto de las transferencias internacionales de datos, corresponde a las empresas exportadoras (que no pueden invocar una evaluación realizada por la Comisión), bajo el control de las autoridades garantes de la UE, que deben autorizar el uso de cláusulas contractuales y las normas corporativas vinculantes para garantizar un nivel adecuado de protección. Dado el alto nivel de protección que el Tribunal ha requerido en el caso *Schrems* para las transferencias internacionales de datos, es muy dudoso que las medidas adoptadas por las empresas por sí solas puedan garantizar este nivel de protección, así como limitar la interferencia de las autoridades públicas de un tercer país. Sobre la importancia de una protección eficaz cuando se transfieren datos personales, debido al aumento exponencial de los flujos de datos, fundamental para la economía digital, y los notables avances en materia de recogida, tratamiento y utilización de los datos, *vid*. Alfonso ORTEGA GIMÉNEZ, Ana MARZO PORTERA (2013), *Empresa y transferencia internacional de datos personales*, Madrid, ICEX Instituto Español de Comercio Exterior, págs. 101; Alessandro MANTELERO (2015), «Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo», en *Il Diritto dell'Informazione e dell'Informatica*, anno XXX, fasc. 4-5, págs. 887-908.

reiterada, los datos personales y la privacidad son dos áreas muy cercanas, pero no idénticas. Prueba de ello es el texto de la Directiva 95/46/CE, en el que ya se planteó la privacidad como condición para el tratamiento de los datos personales, lo que se ha recogido y confirmado en el nuevo RGPD. Por lo tanto, el "*Privacy Shield*" no es un "Escudo" para proteger la privacidad, sino sólo la forma en que se procesan los datos personales. En efecto, una aproximación superficial a este asunto en la que se tome la privacidad y los datos personales como nociones perfectamente intercambiables, conduce a la errónea consideración de que el objetivo del "*Privacy Shield*" es la protección de un derecho absoluto lo que, sin embargo, no es cierto.

180. Como se ha mencionado anteriormente, el 2 de febrero el año 2016 la Comisión Europea anunció el logro de un Acuerdo de principio entre la UE y los EE.UU. en cuanto a las condiciones en las que los datos personales de la UE pueden ser transferidos en este tercer Estado. Este acuerdo fue seguido, el 29 de febrero de 2016, de la presentación por parte de la Comisión de un proyecto de «*Decisión sobre el carácter adecuado de la protección*» de EE.UU.[1157], además de los textos que constituirán el "Escudo de la privacidad UE-EE.UU.". Esto incluye los principios relativos al "Escudo de la privacidad" a los que deben atenerse las empresas y compromisos por escrito del Gobierno de los EE.UU., con garantías relativas a las salvaguardias y limitaciones en materia de acceso a los datos por parte de las autoridades públicas[1158]. Posteriormente, el Grupo de Trabajo anunció su intención de realizar una evaluación de la documentación correspondiente y de adoptar un proyecto de opinión, lo que se hizo en la sesión plenaria de los días 12 y 13 de abril de 2016[1159], a lo que seguría la Resolución del Parlamento Europeo de 26 de mayo[1160]. Después de intensas

[1157] Serena CRESPI (2016).
[1158] COMISIÓN EUROPEA - Comunicado de prensa (2016b), Recuperar la confianza en los flujos de datos transatlánticos gracias a salvaguardias estrictas: la Comisión Europea presenta el Escudo de la privacidad UE-EE.UU., Bruselas, 29 de febrero de 2016. Disponible en Internet: http://europa.eu/rapid/press-release_IP-16-433_es.htm [consulta: 14 de marzo de 2016].
[1159] ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c), Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN, WP 238, Adopted on 13 April 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [consulta: 14 de marzo de 2016].
[1160] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos (2016/2727(RSP)), Bruselas, Jueves 26 de mayo de 2016. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//ES [consulta: 11 de junio de 2016]. En la Resolución, no legislativa, el Parlamento Europeo pidió a la Comisión Europea seguir con las negociaciones con EE.UU. para remediar las faltas del "Escudo de la privacidad". Entre ellas, la falta de independencia y eficaces poderes de la nueva figura del *Ombudsperson* del Estado, la presencia de mecanismos de recurso excesivamente complejos, la capacidad de recopilar grandes cantidades de datos, que en algunos casos podrían entrar en conflicto con los principios de necesidad y proporcionalidad.

negociaciones, la Comisión culminó el procedimiento de adopción el 12 de julio de 2016[1161]. Debe recordarse que la adopción del "Escudo de la privacidad"[1162] se llevó a cabo en un período significativo con respecto a la protección de datos personales en Europa, ya que el 14 de abril de 2016, de hecho, se aprobó el "paquete" de reforma de protección de datos[1163].

181. La Comisión Europea, a pesar de las críticas y reservas al texto[1164], adoptó la Decisión de Ejecución (UE) 2016/1250[1165] basada en nuevos principios contenidos en el

[1161] Para un examen sobre la transición del antiguo al nuevo sistema, consulte Alessandro MANTELERO (2016), «From Safe Harbour to Privacy Shield. The "Medieval" sovereignty on personal data», en *Contratto e Impresa/Europa*, núm. 1; Jan BAEVERSTROEM (2016), «Reactions To The EU-US Privacy Shield, The Successor To The Safe Harbour Agreement», en *European Parliamentary Research Service Blog*, april 18. Disponible en Internet: https://epthinktank.eu/2016/04/18/reactions-to-the-eu-us-privacy-shield-the-successor-to-the-safe-harbour-agreement/ [consulta: 21 de septimbre de 2016]; Ernst-Oliver WILHELM (2016), «A Brief History of Safe Harbor», en *International Association of Privacy Professionals*. Disponible en Internet: https://iapp.org/resources/article/a-brief-history-of-safe-harbor/ [consulta: 23 de octubre de 2016].

[1162] Andrea CARRERA MARISCAL (2016), «Lo que debe saber sobre el Escudo de Privacidad entre la Unión Europea y los Estados Unidos», en *International Association of Privacy Professionals*, sep. 22. Disponible en Internet: https://iapp.org/news/a/lo-que-debe-saber-sobre-el-escudo-de-privacidad-entre-la-union-europea-y-los-estados-unidos/ [consulta: 21 de septimbre de 2016].

[1163] Existe una estrecha relación del "Escudo de la privacidad UE-EE.UU." con las disposiciones contenidas en el nuevo RGPD en relación con las trasferencias internacionales de datos. En tal sentido *vid*. *infra* Capítulo V.

[1164] Veintisiete organizaciones de derechos civiles declararon que no consideraban que el Acuerdo "*Privacy Shield*" entre los EE.UU. y la Unión Europea cumpliese con las normas establecidas por el TJUE (vid. sentencia *Schrems*). Sin más reformas sustanciales para asegurar la protección de los derechos fundamentales de los individuos de ambos lados del Atlántico, los grupos consideraban que el nuevo Acuerdo ponía en riesgo a los usuarios, socavaba la confianza en la economía digital y perpetuaba las violaciones de derechos humanos que ya estaban ocurriendo con los programas de vigilancia y otras actividades. *Vid*. «Transatlantic coalition of civil society groups: Privacy Shield is not enough – renegotiation is needed (Privacy Shield Letter by 27 civil society groups)», en *European Digital Rights (EDRi)*, march 16, 2016. Disponible en Internet: https://edri.org/transatlantic-coalition-of-civil-society-groups-privacy-shield-is-not-enough-renogitation-is-needed/ [consulta: 14 de octubre de 2016]. Muy crítico también fue el eurodiputado Jan Philipp Albrecht, quien declararó que el nuevo marco produce un vaciamiento del derecho fundamental de la UE a la protección de datos. «EU-US data protection/Safe Harbour», en *The Greens/European Free Alliance*, 02.02.2016. Disponible en Internet: https://www.greens-efa.eu/en/article/eu-us-data-protection-safe-harbour/ [consulta: 14 de octubre de 2016].

[1165] DECISIÓN DE EJECUCIÓN (UE) 2016/1250 DE LA COMISIÓN, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU., *Diario Oficial de la Unión Europea*, L 207, 1.8.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016D1250; EUROPEAN COMMISSION - Fact Sheet (2016), EU-U.S. Privacy Shield: Frequently Asked Questions, Brussels, 12 july 2016. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm [consulta documentos: 11 de agosto de 2016]. Andrus Ansip, vicepresidente de la Comisión responsable del Mercado Único Digital, declaro: «*Hoy hemos aprobado el nuevo Escudo de la privacidad UE-EE.UU. Este Escudo protegerá los datos personales de nuestros ciudadanos y aportará claridad a las empresas. Hemos trabajado mucho junto con todos nuestros socios en Europa y en los Estados Unidos para obtener este acuerdo y para tenerlo lo antes posible. Los flujos de datos entre nuestros dos continentes son esenciales para nuestra sociedad y economía: ahora tenemos un marco sólido que garantiza que dichas transferencias se realicen en condiciones mejores y más seguras».* Věra Jourová, comisaria de Justicia, Consumidores e Igualdad de Género, añadió que: «*El Escudo de la privacidad UE-EE.UU. es un nuevo sistema sólido para proteger los datos personales de los europeos y garantizar la seguridad jurídica a las empresas. Aporta normas más estrictas de protección de datos que se aplican mejor, salvaguardias en cuanto al acceso del Gobierno y un recurso más fácil para los particulares en caso de reclamaciones. El nuevo marco restablecerá la confianza de los consumidores cuyos datos sean transferidos al otro lado del Atlántico. Hemos colaborado con las autoridades europeas de protección de datos, el Parlamento Europeo, los Estados miembros y nuestros homólogos de los Estados Unidos para establecer un sistema con las normas más estrictas para proteger los datos personales*

"*EU-U.S. Privacy Shield*", que entró en pleno funcionamiento el 1 de agosto de 2016[1166], reconociendo así, una vez más, la adecuación del sistema de protección de datos en los EE.UU. El objetivo del Acuerdo es permitir los flujos de datos personales transatlánticos desde la Unión Europea hacia los EE.UU. garantizando, no solamente, un nivel de protección adecuado de los derechos de los ciudadanos europeos, sino también, mecanismos y recursos eficaces en pro de la seguridad jurídica[1167]. El Acuerdo es vinculante para los 28 Estados miembros de la UE, así como para Noruega, Islandia y Liechtenstein.

182. Hay que señalar que el "Escudo de la privacidad" no constituye un acuerdo internacional en el sentido propio[1168], sino que está compuesto por una serie de actos unilaterales adoptados por la Comisión Europea y por el gobierno de EE.UU. destinados a regular las transferencias trasatlánticas de datos. El "Escudo de la privacidad" consiste esencialmente en actuaciones propias del gobierno de EE.UU. (en particular, la Comisión Federal de Comercio y el Departamento de Estado) y en la decisión de adecuación, que es un acto ejecutivo de la Comisión Europea. En comparación con el anterior «*Acuerdo de*

de los europeos». En COMISIÓN EUROPEA - Comunicado de prensa (2016c), La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos, Bruselas, 12 de julio de 2016.

[1166] EUROPEAN COMMISSION (2016), EU-U.S. Privacy Shield fully operational from today, 01/08/2016. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704 [consulta: 29 de agosto de 2016]. La "Decisión de adecuación", notificada el 12 de julio de 2016 a los Estados miembros, entró en vigor inmediatamente. Por parte de los EE.UU., el marco del "Escudo de la privacidad" se publicó en el *Federal Register* (Registro Federal), el equivalente a nuestro Diario Oficial. El Departamento de Comercio de los EE.UU. comenzó a operar el "Escudo de la privacidad". Una vez las empresas hayan tenido ocasión de revisar el marco y de actualizar su cumplimiento, podrán certificarse ante el Departamento de Comercio a partir del 1 de agosto. La Comisión Europea también puso a disposición una guía para los ciudadanos que explica cuáles son sus derechos con respecto de las empresas adherentes al "Escudo de la privacidad" y la forma de ejercerlos. COMISIÓN EUROPEA - Dirección General de Justicia y Consumidores (2016), Guía acerca del Escudo de Privacidad UE - EE.UU., págs. 24. Disponible en Internet: https://www.agpd.es/portalwebAGPD/noticias-inicio/common/pdf/2016/08_agosto/es_es_citizens-guide_en.pdf [consulta: 17 de septiembre de 2016].

[1167] La adopción del "Escudo de la privacidad" es el resultado de importantes negociaciones que empezaron con la Comunicación de noviembre de 2013, de la Comisión Europea donde recordó que «*las transferencias de datos personales son un elemento importante y necesario de la relación transatlántica*», siendo «*parte integrante de los intercambios comerciales entre ambos lados del Atlántico, incluidos los relacionados con los nuevos sectores digitales en crecimiento, tales como las redes sociales o la computación en nube, que implican la transferencia de grandes cantidades de datos de la UE a los Estados Unidos*». Así pues, se estableció un vínculo entre los datos personales transferidos desde UE, las relaciones entre Unión Europea y los EE.UU. y comercio. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Restablecer la confianza en los flujos de datos entre la UE y EE.UU. (2013).

[1168] En primer lugar, nunca se menciona en ninguno de los actos la voluntad de concluir un acuerdo internacional, así como se reconoce en los artículos 12 y 13 de la Convención de Viena. Por otra parte, según la legislación europea, la conclusión de un acuerdo internacional en la materia debe seguir el procedimiento de artículo 218 del TFUE, que prevé también la previa aprobación del Parlamento Europeo. Sobre este punto, vid. Stefano SALUZZO (2016), «Tutela dei dati personali e deroghe in materia di sicurezza nazionale dopo l'entrata in vigore del "*Privacy Shield*"», en *SIDIBlog*. Disponible en Internet: http://www.sidiblog.org/2016/09/13/tutela-dei-dati-personali-e-deroghe-in-materia-di-sicurezza-nazionale-dopo-lentrata-in-vigore-del-privacy-shield/ [consulta: 21 de septiembre de 2016].

"Puerto Seguro", las empresas privadas pueden registrarse voluntariamente al "Escudo de la privacidad" si autocertifican que cumplen con las garantías de protección de datos requeridas por el gobierno de EE.UU.»[1169] (*vid*. *infra*), lo que no impide, sin embargo, que, al no ser obligaciones internacionales, dichos compromisos tengan atribuido un valor puramente político[1170].

183. La Decisión de Ejecución (UE) 2016/1250 de la Comisión que, según la misma, tiene en cuenta los requisitos establecidos por el TJUE en el fallo *Schrems*, encuentra su fundamento jurídico en el apartado 6 del artículo 25 de la Directiva 95/46/CE (ahora artículo 45 del RGPD). Teniendo en cuenta que «*los Estados miembros dispondrán que la transferencia a un país tercero de datos personales,* (…) *únicamente pueda efectuarse cuando,* (…) *el país tercero de que se trate garantice un nivel de protección adecuado*», el artículo 25, apartado 1 de la Directiva[1171], establece que si la Comisión Europea comprueba que un tercer país no garantiza un nivel adecuado de protección (apartado 4) o que si lo garantiza (apartado 6), puede adoptar la decisión de adecuación. El "Escudo de la privacidad" es, de hecho, una decisión de adecuación contemplada en el apartado 6 del artículo 25 de la Directiva 95/46/CE[1172]. Con esa decisión, la Comisión, teniendo en cuenta que el sistema estadounidense no protege los datos personales al mismo nivel de la Unión, sin embargo, reconoce la adecuación de las empresas estadounidenses que deseen importar libremente datos de la UE y se autocertifiquen[1173] respetando las reglas contenidas en la decisión, por lo que no necesitarán ni cláusulas contractuales tipo, ni normas corporativas vinculantes, ni ningún otro tipo de autorización por parte de una autoridad de control europea competente para poder realizar sus transferencias de datos.

[1169] Cristina BLASI CASAGRAN (2017). Desde el 1 de agosto de 2016 las compañías americanas ya pueden adherirse a "*Privacy Shield*" a través del sitio web disponible por el Departamento de Comercio de los EE.UU., éste será responsable de verificar el cumplimiento de las políticas corporativas con los principios de "Privacy Shield". Disponible en Internet: https://www.privacyshield.gov/welcome. De la entrada en vigor del "*Privacy Shield*", 2522 son las empresas estadounidenses que han dado el primer paso hacia la adaptación a la nueva normativa. Entre ellos Microsoft, Google, Facebook, Amazon, *etc*. [consulta: 07 de noviembre de 2017].
[1170] Stefano SALUZZO (2016).
[1171] Debe recordarse que en la Unión Europea existen tres mecanismos de conformidad para las transferencias de datos personales: las cláusulas contractuales tipo, las normas corporativas vinculantes (*Binding Corporate Rules*) y las decisiones de adecuación. *Amplius*, Capítulo V, Transferencias de datos personales a terceros países u organizaciones internacionales, del RGPD.
[1172] Andrea CARRERA MARISCAL (2016).
[1173] El cumplimiento del sistema de autocertificación, reconocido también en el antiguo Acuerdo de "Puerto Seguro", es admisible siempre que el control del cumplimiento de los compromisos adquiridos por las empresas estadounidenses sea realmente efectivo.

184. Por lo tanto, el "Escudo de la privacidad" consiste en un conjunto de principios al que –como fue el "Puerto Seguro"– las compañías estadounidenses pueden adherirse voluntariamente para obtener la certificación que les permita recibir y gestionar los datos personales de la UE[1174]. Además, la adhesión a estos principios también implica estar bajo la jurisdicción de la Comisión Federal de Comercio de EE.UU. El Departamento de Comercio de los EE.UU. lleva a cabo actualizaciones y revisiones periódicas de las empresas participantes, con el fin de garantizar que sigan las normas que ellas mismas han suscrito. De lo contrario, la empresa se expone a sanciones y la retirada de la lista de miembros. La gravedad de esta sanción no tiene que ser subestimada ya que para muchas empresas podría representar un estigma para limitar significativamente la capacidad de operar en Europa[1175].

185. También se ven reforzados otros aspectos como el hecho de que los principios del nuevo "Escudo de la privacidad" incluyan condiciones presentes en el RGPD, no incluidas en el anterior Acuerdo de "Puerto Seguro". En este sentido, el nuevo "Escudo" ha sido objeto de nuevos compromisos con un sistema de supervisión más fuerte de protección eficaz de los derechos individuales. Sin embargo, no se han incoporado cuestiones esenciales como, por ejemplo, que se especifiquen en el texto los derechos de los interesados[1176], es decir,

[1174] DECISIÓN DE EJECUCIÓN (UE) 2016/1250, apartado 26.

[1175] Las empresas certificadas gozarán de un reconocimiento de sus políticas de privacidad y de los procedimientos de tratamiento y procesamiento de datos personales implementados en el interior de las mismas. Para esto las empresas interesadas deberán presentar, y están obligadas a publicar en su sitio web, una "*privacy policy*" que esté totalmente en conformidad con los principios previstos en la Decisión de adecuación y deberán prever una cláusula en donde se exprese clara y públicamente que dicha empresa forma parte del "Escudo de la privacidad". Deberán informar a las partes interesadas acerca de la finalidad por la cual utilizan y transfieran los datos personales, el derecho a acceder a sus datos, la posibilidad de arbitraje obligatorio previsto por el Escudo, la posibilidad que los datos recogidos sean comunicados a las autoridades estadounidenses bajo su solicitud, y responsabilidad de la empresa adherente en el caso de una transferencia posterior de los datos a terceros. Dicha política deberá ser clara, comprensible y fácilmente accesible. Las entidades pueden usar la información sólo en relación con los fines para el que fue recogido o autorizada posteriormente por el particular. En el caso de que se quiera utilizar «*para un propósito sustancialmente distinto del objetivo inicial*», el "Escudo de la privacidad" no requiere la aplicación de un nuevo consenstimiento, ya que es suficiente proporcionar a los particulares «*mecanismos claros, visibles y de fácil acceso para que ejerzan su derecho de opción*» ("exclusión"). DECISIÓN DE EJECUCIÓN (UE) 2016/1250, Anexo II, II. Principios, 2. Opción. El principio de elección dispone que las personas deberán tener la posibilidad de oponerse a que sus datos personales sean transmitidos a un tercero o que sean el objeto de un tratamiento ulterior. Sólo si se trata de datos sensibles, la opción de participar será afirmativa o expresa ("aceptación"). Las mismas reglas se aplican en el caso de la divulgación de datos a terceros. Si la información: «*i) va a revelarse a un tercero, o ii) va a utilizarse para un fin distinto para el que se recogió inicialmente o se autorizó con posterioridad mediante la aceptación del interesado*». Andrea CARRERA MARISCAL (2016).

[1176] Según el considerando 26 de la Directiva (UE) 2016/680 y artículo 5 del RGPD, los datos personales que se recogen no pueden conservarse más tiempo de lo estrictamente necesario para la finalidad por la que fueron recogidos. De manera similar, la Decisión de Ejecución (UE) 2016/1250 en su apartado 23 incorpora disposiciones sobre el «*principio de integridad de los datos y de limitación de la finalidad*». De todos modos, el Grupo de Trabajo ha recomendado que los acuerdos deberían definir de manera más precisa los periodos de conservación en relación con la finalidad perseguida. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2016d), Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, 26 de julio de 2016.

cómo los individuos pueden ejercer sus derechos de acceso, rectificación, modificación y cancelación de sus datos, así como la forma de presentar una reclamación[1177], que no se equipara a los contenidos en las normas europeas[1178].

186. El Anexo II, Síntesis I, punto 5 del "Escudo de la privacidad" prevé la posibilidad de establecer unas excepciones a los principios aplicables al tratamiento de los datos personales cuando: «*a) exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que origine conflictos de obligaciones o prevea autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios está limitado en la medida necesaria para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; o c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables*».

187. Sobre estos puntos existen una fuerte preocupación sobre el cumplimiento de la legislación europea. En particular, las críticas se centran en ciertas garantías que deben acompañar a las injerencias en los derechos fundamentales, para que éstas puedan resultar admisibles[1179]. Estas garantías se aplican a todos los casos de injerencia en el disfrute del

[1177] El principio de notificación e información basado en la transparencia y la exactitud de la información que las empresas deberán comunicar a los titulares de derechos. DECISIÓN DE EJECUCIÓN (UE) 2016/1250, Anexo II, II. Principios, 1. Notificación. Sin embargo, cualquier ciudadano que considere que sus datos se han utilizado de forma indebida en el nuevo sistema del "Escudo de la privacidad" se beneficiarán de varios mecanismos de resolución de litigios "accesibles y asequibles". En este sentido, se permite a los ciudadanos europeos presentar reclamación directamente o a través del Departamento de Comercio de EE.UU. a las empresas estadounidenses, que deben responder al interesado de la UE en un plazo de 45 días; o se ofrecerán gratuitamente mecanismos de resolución alternativa de litigios (*ADR*, por su sigla en inglés). Además, ahora se «*facilita a los interesados una serie de posibilidades para hacer valer sus derechos, presentar reclamaciones en relación con el incumplimiento por parte de entidades autocertificadas*» de los EE.UU., «*y que se resuelvan sus reclamaciones, en su caso mediante una decisión que conceda la tutela judicial efectiva*». *Vid*. apartados 41 a 45 de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250. Concretamente, «*si la vulneración por parte de una compañía estadounidense registrada en el "Escudo de la privacidad" persiste, los ciudadanos europeos tienen un mecanismo alternativo a través de un panel de autoridades de protección de datos establecido en la UE. Este mecanismo se creó con el fin de cumplir con la sentencia del TJUE en el asunto Schrems*». Por ello, en el nuevo Acuerdo, las autoridades nacionales de protección de datos «*proporcionan un mecanismo de recurso independiente que permite investigar quejas contactando con la empresa y buscando la medida compensatoria más justa*». Cristina BLASI CASAGRAN (2017: 197-198).

[1178] Cristina BLASI CASAGRAN (2017: 206).

[1179] Aunque reconoce los esfuerzos realizados para desarrollar una solución para reemplazar el "*Safe Harbor*", el SEPD denunció que el "Escudo de la privacidad", tal como está, no parece lo suficientemente robusto como para soportar el futuro escrutinio legal ante el TJUE. EL SEPD exigía mejoras significativas para respetar la esencia de los principios fundamentales de la protección de datos, especialmente en lo que respecta a los mecanismos de necesidad, proporcionalidad y reparación. Además, reclamaba una solución a más largo plazo en el diálogo transatlántico. Para que el "Escudo" sea eficaz, debe proporcionar una protección adecuada contra la vigilancia indiscriminada, así como las obligaciones de supervisión, transparencia, reparación y protección de datos. De este modo, el SEPD instaba a los legisladores a que se tomen su tiempo para encontrar una solución

derecho a la intimidad y a la protección de datos personales y forman parte del *corpus* regulador conforme al cual la protección otorgada por las leyes de terceros Estados debe ser – según el mecanismo de toma de decisiones de adecuación – sustancialmente equivalente. El Grupo de Trabajo había expresado preocupaciones a este respecto, redactando una lista de requisitos esenciales –conocidas como "*European Essential Guarantees*"– para que el nuevo Acuerdo pudiera considerarse conforme a la legalidad[1180]. Según el Grupo[1181], en unos momentos de creciente inseguridad, debían respetarse los cuatro los pilares para que las interferencias en los derechos fundamentales a la privacidad y la protección de datos como consecuencia de medidas de vigilancia al transferir datos personales pudiesen resultar aceptables, que son: tratamiento basado en reglas claras, precisas y reconocibles; demostración de necesidad y proporcionalidad, en relación con los objetivos legítimos perseguidos; existencia de un organismo independiente, un control eficaz e imparcial del tratamiento[1182]; y, finalmente, la necesitadad de remedios efectivos que permitan a las personas a proteger sus derechos ante el organismo independiente[1183]. Se tratan de garantías

adecuada y a largo plazo. Las empresas internacionales que suministran bienes y servicios en la UE deben tener claridad sobre todas las normas que deben cumplir. EDPS (2016b), Opinion on the EU-U.S. Privacy Shield draft adequacy decisión, Opinion 4/2016, 30 May 2016, págs. 15.

[1180] ARTICLE 29 DATA PROTECTION WORKING PARTY (2016b), Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN, WP 237, Adopted on 13 April 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf [consulta: 11 de septiembre de 2016]. En este mismo sentido, vid. Wojciech R. WIEWIÓROWSKI (2017: 172-173).

[1181] «*No se encuentra ninguna limitación específica en el "Escudo de la privacidad" en cuanto a decisiones basadas en tratamientos automatizados, así que los individuos cuyos datos sean tratados por compañías registradas en el "Escudo de la privacidad" no tienen garantía alguna u opciones de impugnar el procesamiento de datos llevados a cabo sin intervención humana*». Cristina BLASI CASAGRAN (2017). ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c: 18); EDPS (2016a), Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, Opinion 1/2016, 12 February 2016, pág. 14.

[1182] El principio de limitación de finalidad, como es sabido, es la base de las normas europeas de protección de datos (*vid*. artículo 5, apartado 1, letra b), del RGPD y artículo 4, apartado 2, de la DIRECTIVA (UE) 2016/680). «*Es cierto que el "Escudo de la privacidad" regula este principio, pero solamente en relación con los responsables del tratamiento. En cambio, si una compañía recoge datos para una finalidad concreta y luego los transfiere a un encargado del tratamiento, esa empresa encargada del tratamiento no necesita cumplir con la finalidad originaria por la cual los datos personales fueron obtenidos*». Cristina BLASI CASAGRAN (2017). ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c: 22); ARTICLE 29 WORKING PARTY (2016d).

[1183] Si bien destacaba el fortalecimiento significativo de la protección de datos personales de la UE transferidos en EE.UU. con respecto al "Puerto Seguro" de 2000, el Grupo de Trabajo señaló que la propuesta de decisión debería haber simplificado o aclarado el sistema de recursos a los que pueden acceder los individuos de la UE en caso de que consideren violados sus derechos y reglas del Escudo por las empresas estadounidenses, que deberían estar en manos de las autoridades garantes de la UE. Con este fin, el Grupo propuso que estas autoridades de la UE se conviertan en el punto de contacto natural para que los individuos de la UE puedan hacer valer sus derechos. Entre otras aclaraciones solicitadas se encuentran la introducción de un principio más preciso sobre los límites a la conservación de datos, que es la regla de que la empresa puede conservar los datos durante más tiempo del necesario con respecto de los fines para lo cual se llevó a cabo el tratamiento, y la previsión de garantías específicas para la elaboración de perfiles de datos personales. En lo que respecta con el acceso de los datos por parte de las autoridades estadounidenses, el Grupo se manifestó sobre la poca

extraídas de la jurisprudencia del TJUE y del TEDH, centrándose en el respeto al principio de legalidad, en cumplimiento de las excepciones a los criterios de necesidad y proporcionalidad, y sobre la existencia de mecanismos de protección adecuados (no necesariamente legales) para "garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".

188. Como puede comprobarse, también aquí existen excepciones por razones de seguridad nacional, lo que parece ser un factor común en la legislación de protección de datos. Por lo tanto, «*los datos recogidos y tratados por los servicios de inteligencia de los EE.UU. no se encuentran dentro del alcance del "Escudo de la privacidad" que incluye amplias derogaciones cuando las agencias de seguridad solicitan datos a las empresas privada*s»[1184].

189. No obstante, parece que se ven reforzados otros aspectos en tanto los principios del nuevo "Escudo de la privacidad" incluyen exigencias presentes en el RGPD y en la Directiva (UE) 2016/680, no incluidas en el anterior Acuerdo de "Puerto Seguro". Así, por ejemplo, en el anterior "Puerto Seguro" las transferencias ulteriores no estaban prohibidas y los datos podían seguir transfiriéndose sin el consentimiento del usuario una vez recibidos por la empresa estadounidense (a los ciudadanos europeos se les daba la posibilidad de objetarse a dicho tratamiento solamente en casos muy puntuales). En particular, los principios expresados en el nuevo "Escudo de la privacidad" y las excepciones concedidas revelan problemas en cuanto a las transferencias ulteriores de datos a un país distinto del país de destino. El endurecimiento de las condiciones para las transferencias ulteriores implica que el destinatario del tercer Estado debe demostrar «*el mismo nivel de protección que los principios*» del "Escudo de la privacidad"[1185]. Con arreglo al «*principio de responsabilidad*»[1186], el encargado del tratamiento deberá, contractualmente, asegurar que una eventual transferencia a un tercero gozará de las mismas garantías y obligaciones exigidas por el "Escudo de la privacidad", lo que incluye el requisito de que «*la aplicación*

independencia del *Ombudsperson* (Defensor del Pueblo), y sobre el efectivo ejercicio e impacto de sus poderes. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c).

[1184] Cristina BLASI CASAGRAN (2017).

[1185] *Vid*. Anexo II de la Decisión de Ejecución (UE) 2016/1250. Tanto el RGPD como la Directiva (UE) 2016/680 requieren que las transferencias ulteriores a terceros Países y organizaciones internacionales cumplan con las normas europeas de protección de datos. *Vid*. RGPD, considerando 101 y artículo 35 de la DIRECTIVA (UE) 2016/680.

[1186] Apartado 28 de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250.

de los principios se limite únicamente a la medida necesaria a efectos de la seguridad nacional, la actuación policial y otros fines de interés público»[1187]. Sin embargo, si este conjunto de reglas, previstas para el tratamiento de datos personales con fines comerciales, también se aplica a la transferencia de datos a terceros países en los que tales datos serán recogidos como parte de las actividades de inteligencia[1188]. La cuestión se materializa en la identificación de las excepciones relativas a la protección de la seguridad nacional en el caso de las transferencias ulteriores[1189].

190. Sin embargo, no está claro cuáles son las reglas aplicables en los casos en que una administración pública de EE.UU. acceda a los datos originarios de la UE y luego, en el contexto de una cooperación para la investigación o inteligencia, transfiera dichos datos a las agencias de los Estados terceros[1190]. Debido a la falta de una determinada regla y la imposibilidad de una aplicación por analogía, en tanto la transferencia no tiene lugar entre privados, queda por determinar si en este caso existen obligaciones vinculantes para las autoridades públicas de los EE.UU. Alguna indicación en este sentido llega del "Acuerdo entre EE.UU.-UE sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales" (*amplius infra*). El artículo 7 de este Acuerdo[1191], precisamente, disciplina el caso de transferencia ulterior, cuando una autoridad competente de una parte le haya transferido los datos personales relativos a un caso específico a una autoridad competente de la otra parte, «*dicha información podrá transferirse a un Estado que no esté obligado por el presente Acuerdo o a un organismo internacional únicamente cuando se haya obtenido el consentimiento previo de la autoridad competente que envió inicialmente los datos*». A la hora de dar su consentimiento a una transferencia, la autoridad competente que transfiere la información

[1187] Véase Anexo II, Sec. I.5 de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250.
[1188] Stefano SALUZZO (2016).
[1189] En el caso de que una organización estadounidense haga una transferencia de datos a operadores privados de terceros países que tengan normas menos estrictas para la recogida de datos personales por parte de las autoridades públicas, según el Grupo de Trabajo, las reglas en materia de transferencias ulteriores deberían encontrar en todo caso aplicación, al menos en el sentido de solicitar, a la organización que transfiere datos de la UE a un tercer país, evaluar el nivel de protección ofrecido por la legislación de ese país y, en su caso, suspender la transferencia, después de informar al titular del tratamiento. Cuando es el mismo responsable del tratamiento de datos UE el que tiene conocimiento del riesgo de una posterior transferencia a un tercer país y autoriza igualmente, o se ve directamente involucrado en la transferencia de datos, la transferencia no se llevará a cabo sobre la base del "Escudo de la privacidad", sino se configurará como transferencia de datos directamente de la UE hacia el tercer país, con reflejo en la disciplina general de los artículos 25 y 26 de la Directiva 95/46/CE. ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c: 20 y ss.).
[1190] Esto es prueba de una forma más tradicional de intercambio de información entre órganos de distintos países, cuya peculiaridad reside en el hecho de que los datos intercambiados están sujetos a un régimen de protección especial, por ejemplo, con respecto a la finalidad o la duración de su almacenamiento.
[1191] *Cfr*. con el siguiente apartado.

en primer lugar tendrá debidamente en cuenta «*todos los factores pertinentes, entre ellos la gravedad de la infracción, el objetivo para el cual se transfirieron inicialmente los datos y si el Estado no sujeto al presente Acuerdo u organismo internacional de que se trate garantiza un nivel adecuado de protección de los datos personales*» (artículo 7, apartado 2).

191. Por lo tanto, tal disposición parece resolver el problema de las transferencias ulteriores, aunque no queda claro[1192] si también se aplica a las actividades de inteligencia o si se pretende regular el intercambio de información sólo en el caso de los procesos penales. No obstante, sigue sin regulación el caso de que los datos hayan sido transferidos desde una entidad privada de la UE a una entidad privada de EE.UU., y después de ser recogidos en territorio estadounidense por la autoridad pública y transferidos a un tercer país. La falta de una norma clara a este respecto despierta, por lo tanto, una importante preocupación, ya que puede convertirse en una herramienta para eludir la disciplina de la normativa europea[1193].

192. Sobre las "obligaciones en materia de transparencia y salvaguardias claras para el acceso de la administración estadounidense" a los datos transferidos desde la UE, EE.UU. ha asegurado oficialmente que el acceso de las autoridades públicas a los datos para fines represivos y de seguridad nacional está sujeto a limitaciones, garantías y mecanismos de supervisión precisos. La novedad es que cualquier persona en la UE tendrá mecanismos de recurso en este ámbito. Los EE.UU. han descartado las actividades de vigilancia masiva e indiscriminada de los datos personales transferidos a los EE.UU. bajo el "Escudo de la privacidad". De acuerdo con la información proporcionada por escrito por la Oficina del Director de Inteligencia Nacional[1194], la recogida de datos en bloque con el tiempo se permitirá sólo bajo ciertas condiciones, y en todo caso serán específicamente predeterminadas y tienen que ser lo más concretas y precisas posible, en el sentido fijado en la *Presidential Policy Directive 28* (*PPD-28*)[1195] introducida por el presidente Obama en

[1192] En Stefano SALUZZO (2016).
[1193] Habría sido más apropiado confiar la tarea de consentir transferencias ulteriores a las autoridades europeas competentes en materia de protección de datos en lugar de a las autoridades responsables de la seguridad, menos sensibles a la protección del derecho fundamental a la protección de datos y más inclinadas a mejorar los requisitos de seguridad. Douwe KORFF (2015), «EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff», en *European Area of Freedom Security & Justice-FREE Group*, 14 October. Disponible en Internet: https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/ [consulta: 14 de enero de 2016].
[1194] Office of the Director of National Intelligence, Office of General Counsel, *Annex VI*, Washington, DC 20511, 22 de febrero de 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf [consulta: 19 de junio de 2016].
[1195] THE WHITE HOUSE - Office of the Press Secretary, Presidential Policy Directive - Signals Intelligence Activities, January 17, 2014. Disponible en Internet: https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [consulta: 19 de junio de 2016].

2014 precisamente para establecer las condiciones de acceso y uso de los datos por parte de las agencias de inteligencia norteamericanas[1196]. Tales limitaciones relativas no sólo a la recopilación, sino también al tratamiento y la difusión de datos, tendrán que, en la práctica, evitar el acceso generalizado a los datos. La Oficina explicó en detalle las salvaguardias existentes en el uso de los datos en estas circunstancias excepcionales[1197]. El Secretario de Estado de EE.UU. ha puesto en marcha dentro el Departamento de Estado un mecanismo de recurso para los europeos para cuestiones relacionadas con la inteligencia nacional a través de la figura del Defensor de los Titulares de los Datos[1198] (en inglés, "*Ombudsperson*").

193. El *Ombudsperson* es nombrado por el Departamento de Estado de los EE.UU.[1199] y «*se encarga de examinar posibles vulneraciones de los derechos de privacidad y protección de datos por parte de las autoridades estadounidenses*». Para ejecutar sus funciones, el *Ombudsperson* «*debe tener conocimiento de las actividades que realizan tanto agentes de policía como servicios de inteligencia de los EE.UU.*». También «*revisa las quejas que se interpongan ante estos organismos públicos, realizando funciones de intermediario entre el usuario y las agencias de seguridad estadounidenses*». El "Escudo de la privacidad" incluye el *Ombudsperson* como «*persona encargada de revisar que las excepciones por seguridad nacional cumplan con el criterio de necesidad y proporcionalidad*»[1200].

[1196] La *Presidential Policy Directive 28* (*cfr*. también nota *supra*) establece que la interceptación de las comunicaciones con fines de inteligencia sea siempre en lamedida que sea posible, referida a las personas identificadas y por razones específicas. Este tipo de intercepción no parece plantear problemas importantes, ya que incluso la más reciente jurisprudencia del TEDH ha reconocido la legitimidad, siempre que la existencia de una sospecha razonable respecto a un individuo sea verificable. Además, la persona sometida a la interceptación siempre debe ser identificado o al menos identificable (como demuestra el mismo TEDH en la sentencia *Zakharov contra Rusia*, apartado 264, comentada en el Capítulo I de esta investigación).

[1197] Queda en todo caso alguna duda sobre la *PPD-28*, ya que no especifica las circunstancias en las que la interceptación de las personas no tenga que seguir realizándose. La *PPD-28* también establece que la inteligencia de señales recopilada en bloque sólo puede utilizarse para seis propósitos concretos: «*la detección y el contraataque ante determinadas actividades de potencias extranjeras; la lucha antiterrorista; la lucha contra la proliferación; la ciberseguridad; la detección y el contraataque a amenazas a los ejércitos estadounidense o aliados; y la lucha contra las amenazas criminales transnacionales, incluida la elusión de sanciones*». Anexo VI, Sec. I, letra b), DECISIÓN DE EJECUCIÓN (UE) 2016/1250.

[1198] Apartado 65 de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250. Las autoridades de EE.UU. se han comprometido también a introducir la posibilidad de recurso a las personas de la UE en el campo de la inteligencia y, de hecho, la *Judicial Redress Act of 2015* del 24 de febrero de 2016 tiene como objetivo ampliar los recursos de la *Privacy Act* también para los ciudadanos de la UE. Tal recurso será introducido a una figura de nueva y adecuada creación, o sea, el "*Privacy Shield Ombudsperson*" (Defensor del Pueblo), hasta el 2017 era Catherine Novelli, el cual, aunque parte del Departamento de Estado, es independiente de los servicios de seguridad de Estados Unidos. THE SECRETARY OF STATE, *Annex III*, Washington, February 22, 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf [consulta: 27 de junio de 2016].

[1199] Apartados 116 a 118, de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250. Esta nueva figura ya ha sido criticada ya que se pone en duda su independencia y falta de poderes en la práctica. «EU-US data protection/Safe Harbour», en *The Greens/European Free Alliance*.

[1200] Cristina BLASI CASAGRAN (2017). El *Ombudsperson* es una figura nueva en el ordenamiento jurídico estadounidense y, por ello, sus poderes y funciones han sido cuestionados. Así mismo, es dudosa la independencia formal y absoluta. ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c: 49-50);

194. Por tanto, y como puede comprobarse, a diferencia de la precedente, la Decisión "Escudo de privacidad" se basa en algo más que los compromisos voluntarios de las empresas estadounidenses individuales, sino también en compromisos firmados y en las garantías dadas directamente por las autoridades estadounidenses. Esta innovación es particularmente importante, ya que refuerza el carácter vinculante del sistema[1201] para la transferencia internacional de datos de la UE en los EE.UU. Estos compromisos también deben ser evaluados a la luz de las reformas aprobadas en los EE.UU. después del caso "*Snowden/Datagate*" para poner fin al fenómeno de la vigilancia masiva "generalizado" e "indiscriminado". El *USA Freedom Act* y la *PPD-28,* de hecho, han introducido restricciones específicas sobre el acceso a los datos personales por razones de seguridad nacional y establecen el principio de que la recogida de información por la inteligencia de EE.UU. debe ser lo más centrada posible.

195. En el marco de la revisión conjunta anual[1202], el mecanismo permitirá monitorizar el funcionamiento del "Escudo de la privacidad", incluidos los compromisos y garantías de acceso a los datos con el fin de luchar contra la delincuencia y seguridad nacional. La Comisión Europea y el Departamento de Comercio de los EE.UU. llevarán a cabo el análisis, al que se asociarán expertos de inteligencia estadounidense y las autoridades europeas de protección de datos. Esta previsión da contenido a las directrices del TJUE de la sentencia *Schrems*[1203]. Para dar consistencia a esta declaración de principios, también se establece que dicha revisión periódica se centrará en todos los aspectos del "Escudo de la privacidad", incluidas las relativas al acceso de las autoridades públicas de los EE.UU. a los datos de la

EDPS (2016b: 8-11). En el asunto *Schrems*, recordamos que el TJUE se refirió al artículo 47 de la CDFUE «*para pedir mecanismos de control independientes y medios efectivos de compensación ante un tribunal imparcial en caso de violación del derecho de protección de datos a los ciudadanos europeos en los EE.UU.*» Podemos afirmar que no se encuentra un mecanismo de supervisión externa completamente independiente en el "Escudo de la privacidad". EDPS (2016b).

[1201] Con el fin de dar fuerza jurídica vinculante a los compromisos escritos por las autoridades de Estados Unidos, el "Escudo de la privacidad" establece que los actos sean publicados en el Registro Federal de EE.UU. (*U.S. Federal Register*). Daniel LÓPEZ CARBALLO (2016), «A vueltas con las transferencias internacionales de datos: actualidad y seguridad jurídica», en *Actualidad Jurídica Aranzadi*, 22 de septiembre. Disponible en Internet: http://dlcarballo.com/wp-content/uploads/2016/09/AJA-922.pdf [consulta: 03 de octubre de 2016].

[1202] Apartados 145 a 149, de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250.

[1203] El TJUE, en la sentencia en cita (apartado 76), tras afirmar que el nivel de protección que ofrece un tercer País puede evolucionar, han, de hecho, declarado que «*incumbe a la Comisión, tras adoptar una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión*».

UE. Con este fin, la Comisión se basará en todas las demás fuentes de información disponibles[1204] y presentará un informe público al Parlamento Europeo y el Consejo[1205].

196. Después de la revisión anual y con el fin de dar valor a este nuevo procedimiento, la Comisión Europea ahora también puede iniciar un procedimiento de suspensión parcial o total o derogación de la Decisión (apartado 150). Este poder puede ser utilizado, en particular, si «*el nivel de protección que ofrece el Escudo de la privacidad ya no puede considerarse esencialmente equivalente al de la Unión o que existen indicios claros de que ya no puede garantizarse el cumplimiento efectivo de los principios en los Estados Unidos, o de que la actuación de los poderes públicos estadounidenses competentes en materia de seguridad nacional o de prevención, investigación, detección o enjuiciamiento de infracciones penales no brinda el nivel de protección necesario*». Esta disposición es particularmente importante porque puede desempeñar un papel disuasorio frente a posibles incumplimientos por parte de las empresas y autoridades de Estados Unidos, fomentando también la observancia de las normas del "Escudo de la privacidad".

197. Para los intereses de la UE, el esquema así descrito comporta alguna ventaja respecto del precedente: confiere cierta unidad sistemática para la gestión y evolución de la multiplicidad de contactos y relaciones bilaterales, así como un título habilitante para la implicación práctica de las autoridades de protección de datos[1206].

198. Pese a los avances reconocibles respecto a la situación anterior, subsisten, sin embargo, además de las ya especificadas en este apartado, otras objeciones serias sobre el nuevo régimen jurídico para la transferencia de datos entre la UE y los EE.UU. Por lo tanto, ¿el nuevo "Escudo de la privacidad" es compatible con la normativa europea de protección de datos?

[1204] «(…) *incluidos los informes de transparencia previstos en la USA Freedom Act; los informes públicos elaborados por los servicios estadounidenses de inteligencia nacional, las APD y los grupos especializados en materia de privacidad; y la información publicada en los medios de comunicación o cualquier otra posible fuente. Por otra parte, a fin de facilitar la labor de la Comisión a este respecto, los Estados miembros deben informar a la Comisión de aquellos casos en los que las medidas adoptadas por los organismos encargados de garantizar la observancia de los principios en los Estados Unidos no cumplan su cometido, así como de cualquier indicio de que la actuación de los poderes públicos estadounidenses competentes en materia de seguridad nacional o de prevención, investigación, detección o enjuiciamiento de infracciones penales no brinden el nivel de protección necesario*». Apartado 148, DECISIÓN DE EJECUCIÓN (UE) 2016/1250.
[1205] Apartado 149 de la DECISIÓN DE EJECUCIÓN (UE) 2016/1250.
[1206] Juan Fernando LÓPEZ AGUILAR (2017: 566).

199. En primer lugar, la posibilidad persistente de que las agencias de inteligencia estadounidenses recurran a herramientas de vigilancia masiva, aunque sea en casos específicos, es una cuestión que despierta muchas dudas. El problema en realidad que surge de la lectura de los anexos a la nueva Decisión de 2016, parece ser no tanto el instrumento utilizado para la transferencia de datos en el extranjero, sino más bien la legislación de EE.UU., que autoriza la recogida y el acceso indiscriminado a los datos de los europeos por las autoridades de seguridad estadounidenses ("*bulk collection of data*"), por lo que ninguna compañía estadounidense podría asegurar que el tratamiento de los datos en los EE.UU. garantizace la protección de los datos de los ciudadanos europeos de forma equivalente a la establecida por la normativa europea, con respecto a los principios de necesidad y proporcionalidad[1207]. El nuevo "Escudo" «*sigue sin contener normas precisas sobre la recogida masiva de datos, y tampoco incluye salvaguardas robustas de supervisión y recursos efectivos para posibles lesiones del derecho de protección de datos a ciudadanos europeos*»[1208]. En este sentido, la *PPD-28* reconoce que los elementos de los servicios de

[1207] Las prácticas de vigilancia y supervisión masiva ("*mass surveillance*"), de acceso de los Servicios de Inteligencia a los datos personales, que han venido estableciéndose en los EE.UU. no encuentran ni admiten parangón con la cultura jurídica, política y social imperante en el Derecho Europeo, tanto en el que emana de fuentes jurídico-comunitarias como en el que caracteriza a los Derechos nacionales de los Estados miembros. En Juan Fernando LÓPEZ AGUILAR (2017: 567). En Europa, se prevé la protección contra el trato ilícito en el sentido de que sólo se necesita consenso para la recopilación de datos, mientras que en los EE.UU. la protección se limita al uso de datos, por lo que la recopilación puede ser indiscriminada o casi donde los límites se refieren sólo al uso posterior de los datos en sí. En esta perspectiva, para los estadounidenses, una recopilación indiscriminada de datos no es una vigilancia masiva (porque no es un procesamiento de datos), donde la vigilancia (y por lo tanto los límites a ella) sólo se discute en el momento de su uso.

[1208] Cristina BLASI CASAGRAN (2017). La vigilancia masiva, sigue siendo una prioridad para los estadounidenses y que el "*Privacy Shield*" no parece abordar de manera concreta. Por ejemplo, la reciente *Cyber Security Act* (Ley de Seguridad Cibernética) que proporciona la transferencia secreta de datos de las compañías web al gobierno de los EE.UU. *Vid*. S.2588 - Cybersecurity Information Sharing Act of 2014, 113th Congress (2013-2014). Disponible en Internet: https://www.congress.gov/bill/113th-congress/senate-bill/2588 [consulta: 03 de octubre de 2016]. Los recientes cambios normativos en los EE.UU., en particular la *PPD-28*, al imponer restricciones al uso de datos recogidos por personas no estadounidenses, no limita de ninguna manera la recopilación masiva. Por lo tanto, resulta incomprensible como pueden considerarse compatibles las intercepciones masivas con los principios de necesidad y proporcionalidad. Bruno SAETTA (2016c), «Il Privacy Shield non è conforme alla normativa europea», en *BrunoSaetta.it*, 26 abril. Disponible en Internet: https://brunosaetta.it/privacy/privacy-shield-non-conforme-normativa-europea.html [consulta: 05 de octubre de 2016]. En este sentido, algunos miembros del Parlamento Europeo han propuesto la adopción de una Resolución común en la que se afirme que la recopilación masiva de datos no cumple con los requisitos de necesidad y proporcionalidad establecidos en la CDFUE. *Vid*. RESOLUCIÓN DEL PARLAMENTO EUROPEO sobre los flujos transatlánticos de datos (2016/2727(RSP)), 24.5.2016. El "Escudo de la privacidad", como ya se ha comentado, incluye diversos mecanismos frente a la «*vulneración del derecho de protección de datos, lo que puede llevar a confusión y hacer más complicado que los ciudadanos europeos decidan iniciar un procedimiento ante compañías estadounidenses. Ninguna de las opciones que se ofrecen a los ciudadanos europeos son directamente ejecutables*». Jan-Philipp ALBRECHT, Max SCHREMS (2016), «Privacy Shield: The new EU rules on transatlantic data sharing will not protect you», en *The Irish Times*, 12 de Julio. Disponible en Internet: http://www.irishtimes.com/opinion/privacy-shield-the-new-eu-rules-on-transatlantic-data-sharingwill-not-protect-you-1.2719018 [consulta: 06 de octubre de 2016]. A pesar de las críticas, por primera vez se sitúa en pie de igualdad el derecho de los ciudadanos estadounidenses a recurrir ante el sistema jurisdiccional europeo y el derecho de los europeos a acudir ante los tribunales de EE.UU. cuando defiendan su derecho de acceso a sus datos personales, rectificación o revelación ilícita y lesiva de su privacidad.

inteligencia «*deberán recopilar la inteligencia de señales en bloque en determinadas circunstancias con el objeto de identificar las amenazas nuevas o emergentes y otra información vital de seguridad nacional que a menudo se esconde dentro del enorme y complejo sistema de las comunicaciones globales modernas*»[1209].

200. En atención a todo este escenario, parece oportuno preguntarse si realmente el "Escudo" es compatible con el artículo 8 de la CDFUE, según la interpretación restrictiva por el TJUE en el caso *Schrems*. Ahora bien, aunque la nueva normativa contiene muchas características nuevas en comparación con la Decisión "Puerto Seguro" y crea un sistema con un mayor nivel de protección de los datos de la UE que el anterior, no es fácil predecir si el régimen establecido podría superar una prueba de dicha compatibilidad ejercida por el TJUE[1210]. Teniendo en cuenta que el "Escudo de la privacidad" no asume la totalidad de las exigencias de la legislación de la UE –que se refuerza aún más con el nuevo RGPD con respecto a la Directiva 95/46/CE– y que los sistemas de la UE y de EE.UU. son diferentes entre sí en este ámbito, resulta difícil afirmar que la nueva Decisión se ajuste a lo exigido en la sentencia *Schrems*[1211].

201. Si bien es cierto que la nueva Decisión también eleva el nivel general de los compromisos aplicables a las empresas estadounidenses que deseen transferir datos desde la UE, aproximando así el sistema previsto en el mismo a las normas europeas[1212], el "*Privacy Shield*" es jurídicamente débil al igual que el "Puerto Seguro" y, por lo tanto, no sería de extrañar que tuviera el mismo fin ante un pronunciamiento del TJUE dando inicio a un nuevo

[1209] Anexo VI, Sec. I, letra b), DECISIÓN DE EJECUCIÓN (UE) 2016/1250. Presupone una recopilación de datos sustancialmente exploratorios, tanto que se admite la recogida a gran escala. Esto también se confirma por el hecho de que la *PPD-28* permite el uso de la recopilación masiva de datos para facilitar las interceptaciones individuales.

[1210] Hasta ahora, de hecho, los tribunales de la UE nunca han tenido ocasión de pronunciarse sobre la totalidad del sistema de transferencia de datos de la UE en los EE.UU. En el caso *Schrems*, el Tribunal centró su atención sólo en algunos aspectos, relacionados principalmente con el acceso a los datos de la UE por las autoridades de EE.UU. por razones de seguridad nacional.

[1211] En particular, apartados 71 («*No obstante, según resulta de los mismos términos del artículo 25, apartado 6, de la Directiva 95/46, esta disposición exige que un tercer país «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. Por otro lado, también conforme a esa disposición, el carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar «a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas»*) y 73 («*Es verdad que el término «adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo,* (…) *debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría*»), de la sentencia *Schrems* del TJUE.

[1212] Serena CRESPI (2016).

"*Schrems* II"[1213]. Debe recordarse que el TJUE anuló el "Puerto Seguro" por su incapacidad de proteger de las "intrusiones" de las agencias de inteligencia en los datos personales de los ciudadanos europeos almacenados en un servidor (*Facebook*) sujeto a la jurisdicción de EE.UU.[1214].

202. En este sentido, el 6 de abril de 2017, la sesión plenaria del Parlamento Europeo respaldó una resolución no legislativa[1215] por la que se pide a la Comisión Europea que realice una evaluación exhaustiva del "*Privacy Shield*"[1216], que garantice a los ciudadanos

[1213] Andrea MONTI (2016), «Privacy Shield: i nodi irrisolti (e irrisolvibili)», en *AgendaDigitale.eu*, 15 luglio. Disponible en Internet: http://www.agendadigitale.eu/egov/privacy-shield-i-nodi-irrisolti-e-irrisolvibili_2374.htm [consulta: 08 de octubre de 2016]. A tal propósito, un nuevo recurso se cierne sobre el "*Privacy Shield*". Dos asociaciones francesas han cuestionado el nuevo Acuerdo ante el TJUE. Se trata de *La Quadrature du Net*, es decir, el proveedor de servicios de Internet sin ánimo de lucro *French Data Network* y la asociación sectorial *Federation FDN*, que solicitan anular (según el artículo 263 del TFUE) la Decisión de la Unión Europea de aplicar el nuevo "Escudo de la privacidad" continuando así con el procedimiento judicial iniciado un mes antes por la ONG *Digital Rights Ireland* contra la Comisión Europea que pretende romper el "Escudo de la privacidad". *Vid*. RECURSO INTERPUESTO el 16 de septiembre de 2016 - Digital Rights Ireland/Comisión, asunto T-670/16, *Diario Oficial de la Unión Europea*, C 410, 7.11.2016; RECURSO INTERPUESTO el 25 de octubre de 2016 - La Quadrature du Net y otros/Comisión, asunto T-738/16, *Diario Oficial de la Unión Europea*, C 6, 9.1.2017. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62016TN0738 [documentos consultados: 28 de enero de 2017].

[1214] El resultado de la disputa parece bastante más incierto si el control ejercido por el TJUE va tan lejos como para controlar el contenido de una ley extranjera, valorando si la ley de EE.UU. ofrece las garantías suficientes a la luz de los criterios de proporcionalidad y necesidad reconocidos en la legislación europea. De hecho, el problema que planteó el fallo *Schrems* es que la Directiva 95/46/CE se aplica al tratamiento de datos personales a un sector (de la seguridad nacional) que se encuentra expresamente fuera del ámbito de aplicación de la Directiva misma. Pretende regular la política interna de un Estado soberano con un instrumento jurídico que, sin embargo, fue diseñado para regular el tratamiento de los datos personales en un marco puramente legal. El uso de un método de interpretación de este tipo, sin embargo, probablemente expondría a la legislación de la UE a la crítica de la "expansión extraterritorial". A este respecto resulta interesante hacer mención a la sentencia del TJUE (Gran Sala), *Yassin Abdullah Kadi y Al Barakaat International Foundation contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas*. El Tribunal establece la proporción de las relaciones entre el orden jurídico comunitario y el sistema jurídico internacional y, en particular, aborda el delicado tema de los efectos que las Resoluciones del Consejo de Seguridad provocan en el ordenamiento jurídico comunitario. En la sentencia *Kadi* los jueces observaron que «*la Comunidad Europea es una comunidad de Derecho, ya que ni sus Estados miembros ni sus instituciones pueden sustraerse al control de la conformidad de sus actos con la carta constitucional fundamental que constituye el Tratado y este último ha establecido un sistema completo de vías de recurso y de procedimientos destinado a encomendar al Tribunal de Justicia el control de legalidad de los actos de las instituciones*» (apartado 281). No hace falta decir que, en ningún caso, un acuerdo internacional puede afectar al sistema de poderes establecidos en el Tratado UE o la autonomía del ordenamiento jurídico europeo (apartado 282). El TJUE reitera el papel desempeñado por los derechos fundamentales: constituyen un requisito de legalidad de los actos comunitarios y que no pueden admitirse en la Comunidad medidas incompatibles con el respeto de los derechos humanos, y también representan un requisito de legalidad de los actos comunitarios (apartados 284 y 285). Sobre estas bases, por tanto, el Tribunal considera que los requisitos impuestos por una orden internacional no pueden de ninguna manera comprometer o socavar los principios constitucionales del Tratado CE, uno de los cuales es sin duda el principio de que todos los actos comunitarios deben respetar los derechos fundamentales.

[1215] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 6 de abril de 2017, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. (2016/3018(RSP)).

[1216] El Grupo de Trabajo dio a conocer las recomendaciones dirigidas a la Comisión Europea en vistas a la primera revisión conjunta del Acuerdo "*Privacy Shield*" sobre la transferencia de datos de la UE a los EE.UU. En lo que respecta a los aspectos relacionados con la aplicación de la ley y la seguridad nacional, el Grupo pedirá garantías sobre el cumplimiento de los principios de necesidad y proporcionalidad en la posible recopilación masiva de datos personales, así como sobre el nombramiento de los cuatro miembros de la *Privacy and Civil Liberties Oversight Board* (que trata de la protección de la privacidad y las libertades fundamentales

europeos el contenido de la CDFUE y las nuevas normas de la Unión Europea en materia de protección de datos. Aunque se reconocen las mejoras significativas en comparación con el viejo Acuerdo UE-EE.UU., hay claras deficiencias que aún deben resolverse para proporcionar seguridad jurídica a los ciudadanos y las empresas que dependen de este nuevo Acuerdo. Entre los eurodiputados hay una gran preocupación por las nuevas medidas adoptadas por la administración americana sobre la privacidad[1217], lo que permite a la *NSA* compartir enormes cantidades de datos privados recabados sin orden judicial, resoluciones judiciales o autorización del Congreso, con otras 16 agencias, incluido el *FBI*, la Agencia Antidroga Norteamericana y el Departamento de Seguridad del Territorio Nacional[1218].

203. A continuación, la Comisión publicó, el 18 de septiembre de 2017, su primer Informe anual sobre el funcionamiento del "Escudo de la privacidad UE-EE.UU.", para determinar que se ha cumplido, "de hecho y de derecho", con todos los aspectos contenido en el Acuerdo. Según el Informe[1219], el "Escudo de la privacidad" continúa asegurando "un nivel adecuado de protección de los datos personales transferidos desde la UE a las empresas

en las actividades del gobierno estadounidense en la lucha contra el terrorismo), sobre el nombramiento del Ombudsperson y los procedimientos que rigen su funcionamiento. ARTICLE 29 DATA PROTECTION WORKING PARTY - Press Release (2017), Preparation of the Privacy Shield annual Joint Review, 13 June 2017.

[1217] Nos referimos, en particular, al *"Executive Order*" (Orden Ejecutiva) de enero de 2017. THE WHITE HOUSE - Office of the Press Secretary, Executive Order: Enhancing Public Safety in the Interior of the United States, January 25, 2017. Disponible en Internet: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united [consulta: 13 de junio de 2017]. El 25 de enero de 2017 el nuevo presidente de los EE.UU. Donald Trump aprobó una nueva Orden Ejecutiva para "Ampliar la Seguridad Pública en el Interior de los EE.UU., la cual restringe el acceso al territorio estadounidense", y en su artículo 14 limita los derechos de privacidad de todas aquellas personas que no son nacionales de los EE.UU., incluidos los ciudadanos europeos. Este texto ya ha suscitado dudas de adecuación con la legislación europea, y los acuerdos internacionales de protección de datos entre la UE y los EE.UU.

[1218] RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 6 de abril de 2017, punto 23. En la Resolución, se pide a la Comisión que evalúe de inmediato la compatibilidad de estas nuevas normas con los compromisos contraídos por las autoridades estadounidenses en el marco del "Escudo de la privacidad", así como su repercusión en el nivel de protección de la protección de datos personales de los EE.UU.

[1219] La Comisión se comprometió a revisar cada año el "Escudo de la privacidad" para evaluar si continúa «*garantizando un nivel adecuado de protección de los datos personales. Para llevar a cabo la revisión conjunta*», la Comisión tuvo en cuenta sus reuniones con el Departamento de Comercio de EE.UU. y la *FTC*, acompañados, por otros departamentos y servicios que intervienen «*en la aplicación del régimen del "Escudo de la privacidad", así como, en asuntos relacionados con la seguridad nacional*», otros servicios de inteligencia y las contribuciones de una amplia gama de partes interesadas (incluidas empresas y ONG). Las autoridades independientes de protección de datos de los Estados miembros de la UE también participaron en el examen. También, debía participar el Ombudsperson, pero hasta la fecha de hoy el puesto está vacante. INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE–EE.UU., COM/2017/0611 final, Bruselas, 18.10.2017; COMISIÓN EUROPEA - Comunicado de prensa (2017b), Escudo de la privacidad UE-EE.UU.: un primer examen indica que funciona, pero que puede mejorarse, Bruselas, 18 de octubre de 2017. Disponible en Internet: http://europa.eu/rapid/press-release_IP-17-3966_es.htm [consulta: 26 de octubre de 2017].

participantes en los EE.UU."[1220]. Con respecto al acceso a los datos personales por parte de las autoridades públicas de los EE.UU. con fines de seguridad nacional, siguen en vigor las garantías oportunas –en nuestra opinión muy débil– por parte de los EE.UU. Sin embargo, se han reconocidos límites y han propuesto recomendaciones para garantizar que el "Escudo de la privacidad" siga funcionando bien[1221].

204. En junio de 2018, el Comité de Libertades Civiles, Justicia e Interior del Parlamento Europeo (LIBE), ha aprobado una moción por la que propone a la Cámara solicitar a la Comisión que suspenda la aplicación del Acuerdo "*Privacy Shield*", si los EE.UU. no cumplen con el mismo en su totalidad antes del próximo 1 de septiembre, porque no proporciona suficiente protección para los ciudadanos de la UE[1222]. Esta posición del Parlamento ha sido adoptada tras conocerse el alcance del caso *Facebook-Cambridge Analytica*[1223], y la evidencia de que ambas compañías están certificadas bajo el "*Privacy Shield*". Entre las principales preocupaciones de la UE con respecto al "Escudo de la privacidad", están el riesgo de una interpretación demasiado amplia de la «*seguridad nacional*» prevista por los EE.UU. y la persistente falta de claridad y transparencia sobre las modalidades de obtener datos masivos en la red por sin razones especificadas de seguridad por la Agencia de Seguridad Nacional (*NSA*).

[1220] La Comisión asegura que el proceso de certificación funciona correctamente y en la actualidad hay más de 2.400 empresas certificadas por el Departamento de Comercio de EE.UU.

[1221] COMISIÓN EUROPEA - Comunicado de prensa (2017b). Algunas de las recomendaciones son las siguientes: un control más dinámico y periódico, por Departamento de Comercio de los EE.UU., del cumplimiento por las empresas de sus obligaciones en virtud del Escudo de la privacidad; mayor conciencia de los ciudadanos de la UE sobre cómo ejercer sus derechos bajo el "Escudo"; una colaboración más estrecha entre las autoridades responsables de la privacidad (Departamento de Comercio, Comisión Federal de Comercio de los EE.UU., y las autoridades de protección de datos de la UE); preservar la protección de los ciudadanos no estadounidenses prevista por la *PPD-28*.

[1222] *Amplius*, PROPUESTA DE RESOLUCIÓN tras una declaración de la Comisión presentada de conformidad con el artículo 123, apartado 2, del Reglamento interno sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU (2018/2645(RSP)), B8-0305/2018, 26.6.2018.

[1223] La empresa de análisis de datos *Cambridge Analytica* recopiló ilegalmente datos personales de más de 50 millones de usuarios de *Facebook* para apoyar la campaña presidencial de Donald Trump, según la investigación del diario *The New York Times* y el *London's Observer*. El reportaje revela el que sería una de las filtraciones de datos más importantes de la historia de *Facebook*. La empresa utilizó los datos recogidos sin autorización a principios de 2014 para elaborar un programa informático que predijera e influyera sobre las opciones electorales. Se utilizaba *Facebook* para recopilar los perfiles de millones de personas y construir modelos para sacar partido a lo que se sabía de ellos. *Vid.*, «Una consultora que trabajó para Trump robó a Facebook datos de 50 millones de usuarios para influir en las elecciones», en *ABC.es*, 18/03/2018. Disponible en Internet: https://www.abc.es/internacional/abci-trump-robo-facebook-datos-50-millones-usuarios-para-influir-elecciones-201803172343_noticia.html; Pablo DE LLANO (2018), «Una consultora que trabajó para Trump manipuló datos de 50 millones de usuarios de Facebook», en *ElPaís.com*, 18 mar 2018. Disponible en Internet: https://elpais.com/internacional/2018/03/17/estados_unidos/1521308795_755101.html [consultados: 08 de septiembre de 2018].

205. Finalmente, además de un marco de regulación más detallado, en el que se han incluido mecanismos de control de las operaciones de inteligencia cuya configuración todavía plantea algunas dudas en cuanto al cumplimiento de las garantías de imparcialidad e independencia[1224], lo que realmente se necesita es exigir a los EE.UU. un cambio en su legislación mediante la inclusión de formas de protección de los derechos humanos equivalentes a las de la legislación europea. Aunque se ha avanzado para mejorar el Acuerdo, en su forma actual "no proporciona el nivel adecuado de protección requerido por la normativa de protección de datos y por la CDFUE". Las transferencias de datos transatlánticas son vitales para la economía, pero esto no puede impedir que se proteja el derecho fundamental a la protección de datos personales, incluso fuera de la UE. La UE y los EE.UU. deben controlar activamente los datos personales para garantizar altos estándares de protección de datos, y, sobre todo, para evitar abusos por parte de las agencias de seguridad. De todo lo anterior, por lo tanto, se pone de manifiesto la existencia de evidentes conflictos entre el "Escudo de la privacidad" y las normas de protección de datos de la UE. Por lo tanto, podemos apoyar la tesis de quienes afirman que el "*Privacy Shield*" no sería otra cosa que «*the same old agreement in pretty new clothes*»[1225].

3.5.2. Límites del Acuerdo Marco UE-EE.UU. sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales ("EU-US Umbrella Agreement")

206. Para concluir con el análisis del impacto de la sentencia *Schrems*, merece la pena realizar una somera referencia al Acuerdo entre los EE.UU. y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales (en adelante, Acuerdo Marco), que entró en vigor el

[1224] Como se ha adelantado, los ciudadanos pueden ejercitar sus derechos en casos de violaciones de protección de datos por parte de compañías sujetas a este acuerdo a través de la *FTC*, el Departamento de Comercio de los EE.UU., el *Ombudsperson*, un panel de arbitraje y, en algunos casos, los tribunales estadounidenses. El «*número tan elevado de autoridades que operan en territorio estadounidense podría representar un problema en la práctica ya que los ciudadanos europeos pueden tener problemas de comprensión sobre cuando usar cada uno de estos recursos*». En vez de incorporar múltiples actores, hubiera sido una mejor opción que el Acuerdo hubiera previsto un único mecanismo de compensación que facilitara el procedimiento y que tuviera suficiente independencia respecto al gobierno estadounidense, de conformidad con las autoridades de protección de los Estados miembros y el TJUE. Cristina BLASI CASAGRAN (2017); EDPS (2016a: 8).

[1225] Estelle MASSÉ, Amie STEPANOVICH, Drew MITNICK (2016), «Activating the EU-US Privacy Shield: To protect privacy, we need reform, not rebranding», en *accessnow.org*, 4 february. Disponible en Internet: https://www.accessnow.org/activating-the-eu-us-privacy-shield/ [consulta: 05 de junio de 2016].

1 de febrero de 2017[1226].Se trata de un Acuerdo internacional[1227] negociado y acordado por la UE con los EE.UU. para garantizar la protección de datos por parte de las autoridades públicas de los EE.UU. y de la UE en sus actividades de prevención, investigación, detección y persecución de delitos[1228], por lo que abarcaría, en particular, los registros de nombres de los pasajeros (*PNR*) y el programa de seguimiento de la financiación del terrorismo (*TFTP*)[1229].

207. El Acuerdo Marco (en inglés, "*EU-US Umbrella Agreement*"), forma parte de las medidas de cumplimiento del reciente Acuerdo llamado "*Privacy Shield*". El Acuerdo tiene el objeto de «*garantizar un elevado nivel de protección de la información personal que se transfiere en el marco de la cooperación transatlántica en la lucha contra el terrorismo y la delincuencia organizada*»[1230]. Complementa los acuerdos existentes entre UE y EE.UU. al tiempo que ayuda a establecer reglas de protección de datos claras y armonizadas para futuros acuerdos en este campo. En ese sentido, el Acuerdo tiene como objetivo "establecer un marco legal duradero «*para facilitar el intercambio de información*»[1231]. Este es el primer Acuerdo internacional de protección de datos en áreas de cooperación policial y judicial penal contra la delincuencia suscrito por la UE con los EE.UU.

[1226] ACUERDO entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales, *Diario Oficial de la Unión Europea*, L 336, 10.12.2016, págs. 3–13. El Acuerdo ha tenido un largo período de gestación: en 2006 se creó un grupo de contacto de alto nivel, compuesto por funcionarios de la UE y de EE.UU., con el fin de identificar las soluciones más adecuadas para una cooperación más estrecha y eficaz en el intercambio de información sobre la lucha contra la delincuencia. En su informe final de octubre de 2009, el grupo sugirió la adopción de un Acuerdo internacional que obligara a la UE y los EE.UU. a aplicar principios comunes de protección de datos para las transferencias transatlánticas de datos en el ámbito de la lucha contra el crimen. Sobre la base de estas conclusiones, en diciembre de 2010, el Consejo autorizó a la Comisión a entablar negociaciones con los EE.UU. para llegar a un acuerdo al respecto. Las negociaciones, iniciadas el 29 de marzo de 2011, se concluyeron el 8 de septiembre de 2015. En particular, la firma de la Ley de Recurso Judicial de los EE.UU. por el presidente Obama en febrero de 2016 abrió el camino para la firma del Acuerdo Marco UE-EE.UU. el 2 de junio de 2016. *Vid*. EUROPEAN COMMISSION - Statement (2016c), Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting, Amsterdam, 2 June 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-2040_en.htm [consulta: 09 de enero de 2017]. De conformidad con el procedimiento establecido por el artículo 218 del TFUE, la aprobación definitiva del Acuerdo ha necesitado el voto del Parlamento Europeo, que tuvo lugar el 1 de diciembre de 2016 (aprobado con 481 votos a favor, 75 en contra y 88 abstenciones), y la aprobación del Consejo al día siguiente. Como ya se ha mencionado, el Acuerdo entró en vigor el 1 de febrero de 2017 tras la notificación de la conclusión de sus respectivos procedimientos de aprobación interna.

[1227] Al revés que ocurre con el Acuerdo "*Privacy Shield*", el "*Umbrella Agreement*" se cualifica jurídicamente como un Acuerdo internacional entre la UE y los EE.UU. *Vid supra*, Stefano SALUZZO (2016).

[1228] El Acuerdo Marco no se aplica a Dinamarca, Irlanda y Reino Unido.

[1229] El Preámbulo establece que las obligaciones establecidas en el artículo 19 del Acuerdo sobre recursos judiciales se aplicaría con respecto a todas las transferencias que entran en el ámbito de aplicación del presente Acuerdo (por lo tanto, también a los *PNR* y *TFTP*).

[1230] Artículo 1 (Objeto del Acuerdo), apartado 1, del Acuerdo Marco.

[1231] Preámbulo del Acuerdo Marco.

208. El Acuerdo cubre toda la información personal (nombres, direcciones, antecedentes penales) compartida entre las autoridades policiales de los Estados de la Unión y los EE.UU. y establece reglas comunes para la protección de la privacidad. Así que, «*los intercambios de datos entre Europol y la Oficina Federal de Investigación (FBI) quedarían sujetos a este Acuerdo*». Asimismo, si el departamento de policía de un Estado miembro de la UE envía «*datos personales relacionados con una investigación policial al departamento de policía de Nueva York debería seguir las normas de este Acuerdo*». Además, debe tenerse en cuenta que «*los intercambios transatlánticos de datos por parte de servicios de inteligencia quedan excluidos del alcance de este Acuerdo*»[1232].

209. Por lo tanto, el Acuerdo establece obligaciones y derechos vinculantes para sus partes en materia de protección de datos personales en supuestos de transferencia de los mismos en actos de cooperación en la investigación y persecución de los delitos. El "*Umbrella Agreement*" no constituye en sí base jurídica autónoma para la autorización de transferencia de datos personales, sino su objeto es proporcionar garantías adicionales a otros Acuerdos de transferencia de datos anteriormente existentes[1233], desde la premisa asumida de la insuficiencia y límites del nivel de protección anteriormente imperante[1234].

210. El artículo 3 del Acuerdo Marco define su ámbito de aplicación, estableciendo que las garantías previstas se aplican a todos los intercambios de datos en el ámbito de cooperación transatlántica en aplicación de la legislación penal. Incluyen las transferencias efectuadas sobre la base de la legislación nacional, los acuerdos entre la UE y los EE.UU. (por ejemplo, el Tratado de Asistencia Jurídica Mutua entre la UE y los EE.UU.), los acuerdos entre los Estados miembros y los EE.UU. (por ejemplo, por la consolidación de la cooperación en la lucha contra las formas graves de delincuencia y los acuerdos sobre información terrorista) y disposiciones específicas para la transferencia de datos personales por organizaciones privadas para luchar contra la delincuencia (por ej., *PNR* y *TFTP*). Según

[1232] Cristina BLASI CASAGRAN (2017: 200-201).
[1233] Entrevista del eurodiputado Jan Philipp Albrecht. *Vid*. «Più tutele per lo scambio di dati tra Use Ue a fini giudiziari», en *Eunews*, 1 dicembre 2016. Disponible en Internet: http://www.eunews.it/2016/12/01/piu-tutele-per-lo-scambio-di-dati-tra-use-ue-fini-giudiziari/73356 [consulta: 07 de enero de 2017].
[1234] *Vid*. artículo 1, apartado 3, del Acuerdo Marco. El artículo 5 (Efecto del Acuerdo) especifica los conceptos contenidos en el artículo 1, cuyo objetivo es integrar, y no sustituir, las disposiciones relativas a la protección de datos personales contenidas en acuerdos internacionales entre las partes en materia de intercambio de datos para la lucha contra la delincuencia. También dispone que las partes adoptarán todas las medidas necesarias para aplicar las disposiciones del Acuerdo en sus legislaciones internas, con especial referencia a las disposiciones relativas a los derechos de las personas físicas. Este subrayado se hizo necesario ya que en el momento de su firma (septiembre de 2015), los EE.UU. aún no habían adoptado la Ley de Recurso Judicial de 2016.

el apartado 2 del mismo artículo, es claro que los derechos de privacidad y protección de datos personales no son absolutos, y es habitual que las medidas de seguridad nacional permitan excepciones en determinados derechos y libertades civiles. Concretamente, el Acuerdo Marco incluye una excepción que establece que el mismo «*no afecta a las transferencias u otras formas de colaboración*» para aquellas autoridades «*responsables de velar por la seguridad nacional*»[1235].

211. Con respecto a estas excepciones por razones de seguridad nacional, se pueden formular importantes críticas[1236] ya que los datos recopilados y procesados por los servicios de inteligencia de los EE.UU. no están incluidos en el alcance del Acuerdo Marco ni tampoco del "Escudo de la privacidad". Por lo tanto, «*el Acuerdo Marco sólo regula los datos tratados*» por entidades policiales, y, «*por otro lado, el "Escudo de la privacidad" incluye*» amplias excepciones «*cuando las agencias de seguridad solicitan datos a las empresas privadas*»[1237].

212. El Acuerdo Marco, «*igual que el "Escudo de la privacidad"*», incluye una serie de principios fundamentales, «*entre los que se encuentran el principio de limitación de finalidad*» (artículo 6 - Limitación de los fines y de la utilización), que establece que el tratamiento sólo puede realizarse con fines explícitos y legítimos dentro del ámbito del Acuerdo Marco[1238].

213. Uno de los principales resultados de este Acuerdo es la inclusión de normas sobre transferencias ulteriores[1239]. El artículo 7 (Transferencia ulterior) establece la necesidad de un «*consentimiento previo de la autoridad competente*» que envía «*inicialmente los datos*» en caso de transferencias ulteriores, y se requiere que el tercer Estado que recibe la información garantice «*un nivel adecuado de protección de los datos personales*»[1240]. Este principio – que ya se ha mencionado también en el "Escudo de la privacidad" – exige que

[1235] Cristina BLASI CASAGRAN (2017).
[1236] Douwe KORFF (2015); EDPS (2016a: 7 y ss.).
[1237] Cristina BLASI CASAGRAN (2017).
[1238] Cristina BLASI CASAGRAN (2017). El Acuerdo Marco prevé en su artículo 2 (Definiciones) una definición de «*tratamiento de datos personales*» («*cualquier operación o conjunto de operaciones relativas a la recogida, conservación, utilización, modificación, organización o estructuración, difusión o divulgación, o disposición de los datos*») que resulta más afín a la perspectiva europea que a la americana. De hecho, el Acuerdo Marco también describe el tratamiento y recogida de datos como lo es en Europa. Si bien, en realidad, la recogida de datos en los EE.UU. no siempre se considera un tratamiento, al menos hasta que se utilice, a través de la selección, los datos recopilados.
[1239] *Cfr*. apartado de anterior sobre las transferencias ulteriores en el "Escudo de la privacidad".
[1240] Artículo 7 (Transferencia ulterior) del Acuerdo Marco.

las garantías previstas en el Acuerdo Marco no se vean frustradas por la transferencia a un tercer país que no tenga el mismo nivel de protección de los datos personales establecidos en el Acuerdo[1241]. De hecho, la autoridad que lleve a cabo la transferencia original para autorizar dicha transferencia deberá tener en cuenta «*todos los factores pertinentes, entre ellos la gravedad de la infracción, el objetivo para el cual se transfirieron inicialmente los datos y si el Estado no sujeto al presente Acuerdo u organismo internacional de que se trate garantiza un nivel adecuado de protección de los datos personales*» (apartado 2). Asimismo, se incluye en el Acuerdo los principios de proporcionalidad y necesidad que se encuentran recogidos en el mismo.

214. Finalmente, por lo que respecta a la conservación de datos, se prevé que los datos personales no puedan conservarse «*durante más tiempo del necesario y apropiado*» (artículo 12 - Periodo de conservación), permitiendo a las Partes el derecho de especificar en su legislación «*la finalidad del tratamiento, la naturaleza de los datos y la autoridad que la tramita, la repercusión sobre los derechos e intereses de las personas afectadas, y otras consideraciones jurídicas aplicables*»[1242]. Esta disposición está destinada a producir profundas diferencias de disciplina entre las Partes, teniendo en cuenta las considerables discrepancias en los enfoques de los dos lados del Atlántico sobre la idoneidad del período de retención de los datos personales[1243]. En general, las políticas de los organismos

[1241] Como se mencionó, tanto el "Escudo de la privacidad" como el Acuerdo Marco ambos contienen cláusulas de transferencia ulterior de datos. Este es un factor positivo, ya que tanto el RGPD, considerando 101, como la Directiva (UE) 2016/680, artículo 35, «*requieren que las transferencias ulteriores a terceros Países y organizaciones internacionales cumplan con las normas europeas de protección de datos*». Sin embargo, se pueden hacer críticas al respecto: «*si los datos enviados a EE.UU. vía el "Escudo de la privacidad" o el Acuerdo Marco cumplen con las mismas restricciones en materia de transferencias ulteriores que las que establecen las normas europeas de protección de datos. En el caso del Acuerdo Marco, éste solo incluye limitaciones cuando las transferencias ulteriores son a otros terceros Estados, pero aquí no se contemplan los intercambios de datos personales entre agencias estadounidenses. Por ejemplo, si la UE manda datos personales al FBI, no hay restricción alguna en la posibilidad de compartir esos datos con otras agencias de los EE.UU. como la Agencia Antidrogas Estadounidense (DEA)*». *Vid*. Cristina BLASI CASAGRAN (2017: 202-205).

[1242] Como ya se ha mencionado, el TJUE ha anulado la Directiva 2006/24/CE (sentencia *Digital Rights Ireland*), ya que viola el principio de proporcionalidad en el equilibrio entre el derecho a la protección de los datos personales y las exigencias de seguridad pública. Uno de los puntos planteados por el Tribunal en su apreciación de la incompatibilidad de la Directiva con los principios fundamentales de la UE era la duración misma de la retención de datos personales por parte de las empresas de telecomunicaciones, de seis meses a dos años, excesiva por el TJUE y no cumple ningún criterio objetivo para su determinación, de modo que se garantice la conservación de los datos durante el período estrictamente necesario para los fines perseguidos. En consecuencia, dada la rigurosidad impuesta por el TJUE, no cabe duda de que la aplicación de este artículo dará lugar a resultados muy diferentes.

[1243] En el ámbito de la seguridad, se prevé la obligación de adoptar normas de conservación cuyo objeto sea garantizar que los datos personales «*no se conservan durante más tiempo del necesario y apropiado*», sin más especificaciones. Según el Acuerdo Marco, los datos también se pueden conservar durante un período de tiempo que se utilizará en una investigación posterior. «*Las normas europeas garantizan que los datos personales que se recogen no pueden conservarse más tiempo de lo estrictamente necesario para la finalidad por la que fueron recogidos*» (*vid*. considerando 26 de la DIRECTIVA (UE) 2016/680 y artículo 5 del RGPD).

gubernamentales de los EE.UU. proporcionan un período máximo de retención de datos de 5 años 30. Por otro lado, el Acuerdo *PNR* entre los EE.UU. y la UE (vid. *supra*) prevé que se puedan almacenar datos personales durante cinco años en una base de datos activa y durante otros diez años en una base de datos inactiva. Por lo contrario, la mencionada nueva Directiva *PNR* de la UE prevé un período de retención máximo de cinco años y la despersonalización de los datos después de seis meses (*vid. supra*).

215. El nuevo esquema refuerza los derechos de los ciudadanos, y, así, entre los aspectos más importantes, reconoce por vez primera el derecho de acceso a la rectificación y a los recursos judiciales de los ciudadanos europeos ante las autoridades y tribunales de EE.UU. Estas facultades a favor de los individuos resultan novedosas, cuando desde hace mucho tiempo forman parte de los derechos relacionados con el pleno cumplimiento de la protección de datos personales en Europa, hasta el punto de ser requisito mínimo en cualquier legislación de protección de datos cuando se trata de la protección de datos personales en los EE.UU. El derecho de acceso, que consiste en el derecho a solicitar y obtener el acceso a sus datos personales y el derecho de rectificación, que autoriza a toda persona a solicitar la corrección o rectificación de sus datos personales si son incorrectos o han sido tratados incorrectamente. El derecho de acceso de la persona afectada no es absoluto, ya que la autoridad competente tiene la posibilidad de restringir dicho acceso para salvaguardar la «*seguridad pública y nacional*» y «*evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales*»[1244].

De todos modos, el Grupo de Trabajo «*ha recomendado que los acuerdos deberían definir de manera más precisa los periodos de conservación en relación con la finalidad perseguida*». Cristina BLASI CASAGRAN (2017) y ARTICLE 29 WORKING PARTY (2016d).

[1244] Artículo 16 (Acceso), apartado 2, del Acuerdo Marco. Si bien los derechos de "acceso", "corrección o rectificación", "oposición" y "supresión" están regulados en el Acuerdo Marco, éstos están sujetos a amplias excepciones. Por ejemplo, en algunos casos incluye una restricción en el acceso a los datos personales: «*a) proteger los derechos y libertades de los demás, incluida su privacidad; b) velar por la seguridad pública y nacional; c) proteger información sensible a efectos policiales y judiciales; d) evitar que se obstaculicen pesquisas, investigaciones o procedimientos jurídicos u oficiales; e) evitar que se prejuzgue la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales; f) proteger intereses previstos en la legislación en materia de libertad de información y acceso a los documentos*». En este sentido, «*no es fácil pensar en una situación en la que los datos personales tratados para fines de seguridad no puedan ser considerados como información policial sensible por parte de las autoridades competentes*». Por ello, el Grupo de Trabajo y el SEPD sugirieron «*añadir un mecanismo indirecto de acceso a los datos personales por parte de los ciudadanos europeos a través de sus autoridades de protección de datos nacionales equivalente al establecido en el artículo 17 de la DIRECTIVA (UE) 2016/680*». Cristina BLASI CASAGRAN (2017); EDPS (2016a) y (2016b); ARTICLE 29 WORKING PARTY (2016d). Por último, el acceso puede no ser gratuito, ya que sólo se especifica que no se impondrán gastos excesivos.

216. Por otra parte, se reconoce el derecho a cualquier ciudadano de una de las partes a interponer un recurso judicial con respecto a la denegación del acceso a registros que contienen sus datos personales, la denegación por la modificación de los registros que contengan datos de carácter personal que le conciernan, y la divulgación ilícita de tal información de manera intencionada o deliberada, lo que deberá incluir la posibilidad de una indemnización compensatoria[1245]. Este punto ha sido y es uno de los principios más criticados por la doctrina especializada, si bien ha sido acogido de manera satisfactoria por las instituciones europeas[1246]. En efecto, la Ley de Recurso Judicial[1247] de los EE.UU. contiene limitaciones que ponen en duda su certeza como mecanismo de compensación para ciudadanos europeos[1248]: no se contempla la cobertura del derecho de acceso a la tutela judicial de ciudadanos no europeos en defensa de sus datos, pese a que la redacción de los artículos 7 y 8 de la CDFUE configuran su titularidad subjetiva con la mayor extensión reconociendo esos derechos a todas las personas, ciudadanos europeos (por serlo de un Estado miembro) o de cualquier país tercero. La Ley de Recurso Judicial sólo cubre datos transferidos para fines de prevención, investigación, detección y persecución de delitos y sólo cuando los envíe una autoridad europea o nacional (excepto si pertenece a Reino Unido, Irlanda o Dinamarca) a agencias específicas de los EE.UU., o bien de una compañía privada a las autoridades públicas estadounidenses pertinentes. Sin embargo, excluye de su alcance

[1245] Artículo 19 (Recursos judiciales), apartado 1, del Acuerdo Marco. En otros casos, los ciudadanos europeos dispondrán también de recursos administrativos y queja ante una autoridad de supervisión independiente en EE.UU. Artículo 18 (Recursos administrativos) del Acuerdo Marco.

[1246] A este respecto, la Comisaria Europea de Justicia, Derechos Fundamentales y Ciudadanía, Věra Jourová, expresó su plena satisfacion: «*This new law is a historic achievement in our efforts to restore trust in transatlantic data flows. The Judicial Redress Act will ensure that all EU citizens have the right to enforce data protection rights in U.S. courts*». *Vid*. EUROPEAN COMMISSION - Statement (2016a), Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama, Brussels, 24 February 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm [consulta: 23 de octubre de 2017].

[1247] Sobre esta Ley (*US Judicial Redress Act*), *vid*. *supra* los apartados en el que se analiza el "*Privacy Shield*". La introducción de un recurso judicial para los ciudadanos europeos era también un requisito expresamente requerido para la adopción por parte de la UE tanto del "Escudo de la privacidad" como del Acuerdo Marco.

[1248] Entre las críticas a respecto, *vid*. David BENDER (2015), «The Judicial Redress Act: A Path to Nowhere», en *International Association of Privacy Professionals*, Dec. 17. Disponible en Internet: https://iapp.org/news/a/the-judicial-redress-act-a-path-to-nowhere/ [consulta: 19 de enero de 2016]; Francesca BIGNAMI (2015), «The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens», en *Study for the LIBE Committee*, European Parliament, págs. 36; Douwe KORFF (2015); Bruno SAETTA (2016a), «Il Judicial Redress Act non tutela adeguatamente la privacy degli europei», en *BrunoSaetta.it*, 26 Febbraio. Disponible en Internet: https://brunosaetta.it/privacy/il-judicial-redress-act-non-tutela-adeguatamente-la-privacy-degli-europei.html [consulta: 23 de enero de 2016]; Edward HASBROUCK (2016), «The limits of the US Judicial Redress Act» en *Privacy Laws & Business*, issue 140, april, págs. 21-23. Disponible en Internet: https://papersplease.org/wp/wp-content/uploads/2016/02/JudicialRedressAct.pdf [consulta: 23 de octubre de 2017]; Cristina BLASI CASAGRAN (2017: 208-209); Marco MASTRACCI (2017), «L'Accordo quadro tra USA e UE sul trasferimento dei dati personali per il contrasto della criminalità», en *La Comunità Internazionale*, vol. LXXII, núm. 1, págs. 53-54. Disponible en Internet: http://www.mpmlegal.it/public/pubblicazioni/5mastracci.pdf [consulta: 12 de octubre de 2017]; Juan Fernando LÓPEZ AGUILAR (2017: 571 y ss.).

de protección todos los datos conseguidos o recogidos por otros medios, o para autoridades fuera del alcance de la ley (los datos recogidos con fines no policiales; y datos transferidos desde la UE al gobierno estadounidense como intermediarios comerciales en los EE.UU.)[1249]. En otras palabras, no se reconoce a los ciudadanos europeos si sus datos han sido originariamente intercambiados entre compañías privadas y después interferidos por las autoridades estadounidenses. Además, como ya se ha comentado al comienzo de este apartado, los datos recogidos por los servicios secretos de los EE.UU. como la Agencia de Seguridad Nacional (*NSA*) quedan fuera del alcance de esta ley[1250]. Esto es realmente lamentable teniendo en cuenta que el detonante de la decisión *Schrems* fue precisamente la recogida masiva de datos personales de ciudadanos europeos por parte de la *NSA*, situación que sigue sin cambios después de esta reforma.

217. Siguiendo con un análisis más profundo, además de las cuestiones ya apuntadas, surgen numerosas dudas sobre el "*Umbrella Agreement*". Así, se ha discutido desde un principio[1251] el alcance del Acuerdo Marco, así como por el "Escudo de la privacidad", sobre todo por lo que respecta a la conformidad con los Tratados de la UE y las recientes normas europeas de protección de datos[1252]. No se puede sino estar de acuerdo con quienes consideran que este Acuerdo es «*ambiguous way*»[1253] porque, además de las lagunas considerables, también incluye aspectos indudablemente positivos.

218. En primer lugar, las normas son muy vagas y permiten un amplio margen de decisión a las autoridades estadounidenses[1254]. Por ejemplo, la notificación de una violación de la privacidad debe estar en presencia de un «*riesgo importante de menoscabo*», pero sin

[1249] Douwe KORFF (2015).
[1250] Está totalmente excluido del derecho a demandar a las agencias federales para obtener compensación si la retención de datos no respeta los principios de exactitud, pertinencia, puntualidad e integridad en la medida necesaria para asegurar la corrección de determinaciones asumida respecto al individuo. *Vid*. Robert GELLMAN (2014), «Foreigners' privacy rights in the US: Little more than a gesture», en *Privacy Laws & Business*, August, issue 130, págs. 7-9. Disponible en Internet: https://www.bobgellman.com/rg-docs/rg-PL&B-PA-Gesture-14.pdf [consulta: 15 de marzo de 2015]; Franziska BOEHM (2015), «A comparison between US and EU data protection legislation for law enforcement purposes», en *Study for the LIBE Committee*, European Parliament, pág. 72. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf [consulta: 05 de enero de 2016]; Edward HASBROUCK (2016: 22).
[1251] Recordamos: EDPS (2016a) y EDPS (2016b); ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c) y ARTICLE 29 WORKING PARTY (2016d).
[1252] Douwe KORFF (2015).
[1253] En Franziska BOEHM (2015: 72 y 74).
[1254] Por ejemplo, la atribución a las autoridades de EE.UU., incluso de forma acumulativa entre ellos, un papel de supervisión no constituye una garantía suficiente, ya que notoriamente carecen de los requisitos de independencia y la falta de poderes incisivos de los homólogos europeos, con competencias muy limitadas. Franziska BOEHM (2015: 72).

proporcionar ninguna información sobre lo que constituye un daño[1255]. El daño se define, generalmente, como daño económico, por lo que otros tipos de daño (imagen, morales) podrían ser excluidos.

219. El artículo 13 (Categorías especiales de datos personales), apartado 2, del Acuerdo Marco prevé "la posibilidad de realizar transferencias masivas de información sensible entre los Estados Unidos y la Unión Europea o un Estado miembro[1256]. Esta disposición se aparta de los dictámenes emitidos por el SEPD y el Grupo de Trabajo[1257], que habían recomendado que se excluyera la transferencia de datos sensibles del contenido del Acuerdo. Este punto es especialmente preocupante, como también lo fue en el caso del "Escudo de la privacidad", si recordamos que el TJUE sentenció que la vigilancia masiva por parte de los Estados Unidos violó el derecho fundamental de protección de datos y privacidad de la Unión Europea. En este sentido, el artículo 37 de la Directiva (EU) 2016/680 establece que los Estados miembros tienen la posibilidad de "transferir datos personales a un tercer país cuando se preveann garantías apropiadas para la protección de datos personales en un instrumento jurídicamente vinculante".

220. En todo caso, puede calificarse el Acuerdo Marco como un intento "oportuno" de acercar las dos posiciones (EU-EE.UU.) tratando de crear un espacio jurídico común en el que se protejan los datos personales, independientemente del territorio en el que se traten. En efecto, las instituciones de la UE, al contemplar que el acceso de las autoridades policiales a esta cantidad de información entraña un importante riesgo de interferencia excesiva de los gobiernos en la vida de los ciudadanos, han subordinado este poder a través de un creciente conjunto de límites cada vez más detallados. Por lo contrario, será necesario comprobar si el Acuerdo dará lugar a cambios en la perspectiva estadounidense, o seguirán considerando el

[1255] El Acuerdo aborda la cuestión de la seguridad de los datos, prescribiendo que las partes adopten las «*medidas técnicas*», «*organizativas*» y de seguridad «*adecuadas*» para proteger la información personal de la «*destrucción accidental o ilícita*», «*pérdida accidental*» y «*difusión, alteración, acceso u otro tratamiento no autorizado*». Artículo 9 (Seguridad de la información) del Acuerdo Marco. En caso de producirse alguno de los hechos que produzcan un riesgo significativo de daño, deberán tomarse medidas oportunas para mitigar el daño, incluida la notificación a la autoridad competente de trasferencia y, en su caso, las circunstancias del accidente, a la persona en cuestión. Artículo 10 (Notificación de un incidente de seguridad de la información) del Acuerdo Marco.

[1256] Artículo 13 (Categorías especiales de datos personales), apartado 2, del Acuerdo Marco: «*En caso de que los Estados Unidos de América, por una parte, y la Unión Europea o un Estado miembro, por otra, celebren un acuerdo sobre la transferencia de datos personales, excepto en relación con casos, investigaciones o actuaciones judiciales específicos, dicho acuerdo preverá más detalladamente las normas y condiciones en las que tales datos personales puedan ser tratados, teniendo debidamente en cuenta la naturaleza de la información y la finalidad para la que se utiliza*». Marco MASTRACCI (2017: 51-52)

[1257] EDPS (2016b); ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c).

tratamiento en su definición más restrictiva con un enfoque dirigido a permitir la prevalencia en cualquier caso de las necesidades de seguridad de la libertad de circulación de los ciudadanos – en especial los no estadounidenses – mediante la adopción de medidas que permitan a las autoridades policiales acceder a estos datos indiscriminadamente.

221. En fin, el Acuerdo quiere establecer una norma mínima de garantías, que no pueda ser derogada en *peius* con la estipulación de acuerdos futuros entre las partes. El Acuerdo Marco refuerza, aunque con algunas excepciones, los derechos de los ciudadanos europeos como el de "acceso", "corrección o la rectificación", "supresión" y "bloqueo" de sus datos; un "nuevo mecanismo de control"; y reconoce, por vez primera, el derecho que cualquier ciudadano europeo obtenga una indemnización administrativa y judicial en caso de vulneración de sus derechos[1258].

222. En su conjunto, pues, y particularmente en este aspecto, el Acuerdo robustece las garantías disponibles en la estructura ya existente de tratados bilaterales entre la UE o sus Estados miembros con EE.UU., muchos de los cuales habían sido lógicamente concluidos antes de la actualización y extensión del nivel de protección de datos operado por la aprobación definitiva, después de un íter prolongado e intensamente problemático de la reforma de protección de datos de 2016 en la UE[1259]. Además, al mismo tiempo, el "*Umbrella Agreement*" incrementa la cooperación policial y judicial penal, refuerza el Derecho aplicable en ELSJ, y, consiguientemente, la seguridad jurídica en la cooperación transatlántica para la investigación y enjuiciamiento de delitos graves transnacionales y terrorismo.

223. Sin duda resultaba urgente "la necesidad de establecer un marco de protección de datos coherente entre los EE.UU. y la UE", especialmente después de las revelaciones de Snowden y de la anulación del Acuerdo de "Puerto Seguro". Sin embargo, este nuevo régimen entre EE.UU. y la UE no converge completamente con las normas de la UE, ya que el Acuerdo Marco ni siquiera cumple, como ocurre con el "Escudo de la privacidad", con

[1258] Cristina BLASI CASAGRAN (2017). Véase la Ley de Recurso Judicial.

[1259] Además de los condiciones establecidos por el TJUE, la Comisión Europea y las autoridades de EE.UU. tuvieron otro obstáculo a la hora de elaborar el Acuerdo Marco: tenían que armonizarlo con la nueva Directiva (UE) 2016/680. Como ya se ha indicado, la «*Directiva regula el intercambio de datos transfronterizo entre autoridades policiales y judiciales dentro de la UE, así como el tratamiento de datos personales entre entes policiales a nivel interno. Así pues, era imprescindible que cualquier acuerdo internacional relacionado con el intercambio de datos entre entes policiales y judiciales de la UE (como es el caso del "Umbrella Agreement") fuera coherente con las normas de la UE y concretamente con la Directiva (UE) 2016/680*». Cristina BLASI CASAGRAN (2017).

todas las garantías de protección de datos que prevé el RGPD y la Directiva (UE) 2016/680. Es por todas estas consideraciones que existen importantes dudas en cuanto a la capacidad de resistencia del Acuerdo ante un eventual escrutinio por parte del TJUE.

4. ¿*Quis custodiet ipsos custodes*? La sentencia *Tele2 Sverige-Watson* sobre la retención de datos de tráfico con fines de seguridad y orden público

224. Con la sentencia de 21 de diciembre de 2016, el TJUE cierra el círculo (al menos por el momento) alrededor del cual los jueces y legisladores europeos se han movido en los últimos años en busca del "justo equilibrio" entre privacidad y exigencias de seguridad pública[1260].

225. La siguiente frase podría ser utilizada en muchos contextos, pero resulta particularmente práctica para describir la continuidad con la que el TJUE, poco más de un año después de la sentencia *Schrems*, vuelve a pronunciarse sobre el derecho a la privacidad: «*Si los hombres fueran como ángeles, no sería necesario gobierno alguno. Si los ángeles gobernaran a los hombres, no sería necesario ningún control externo o interno sobre el gobierno. Al organizar un gobierno de hombres para hombres, la gran dificultad estriba en esto: primero hay que capacitar al gobierno para que controle a los gobernados; luego hay que obligarle a que se controle a sí mismo*»[1261]. Con esta cita de James Madison[1262], el Abogado General en los asuntos *Tele2 Sverige-Watson* abre sus conclusiones, en un asunto en el que el TJUE, una vez más, se pronuncia sobre la compatibilidad de las normas nacionales sobre retención de datos, es decir, recopilación y conservación de datos de tráfico telefónico y posterior acceso de las autoridades nacionales por razones de seguridad, con la legislación europea.

[1260] Oreste POLLICINO y Marco BASSINI (2017), «La Corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico», en *Diritto Penale Contemporaneo*, págs. 10.

[1261] CONCLUSIONES DEL ABOGADO GENERAL Sr. Henrik Saugmandsgaard Øe, presentadas el 19 de julio de 2016, Asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen* (C-203/15) y *Secretary of State for the Home Department contra Tom Watson, Peter Brice, Geoffrey Lewis* (C-698/15). Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=ES [consulta: 02 de noviembre de 2017]; y el artículo «La obligación de conservación de datos impuesta por un Estado debe estar sujeta a estrictas garantías», en *Law&Trends*, 19/07/2016. Disponible en Internet: http://www.lawandtrends.com/noticias/ue-internacional/la-obligacion-de-conservacion-de-datos-impuesta.html [consulta: 02 de noviembre de 2017]; Oreste POLLICINO y Marco BASSINI (2017).

[1262] James MADISON (2009), «Federalist n. 51», en Alexander HAMILTON, James MADISON, y John JAY, *The Federalist Papers*, ed. Michael A. Genovese, Nueva York, Palgrave Macmillan, pág. 120.

226. Es decir, ¿hasta qué punto los Parlamentos pueden adoptar normas sobre retención de datos en tiempos de "terrorismo ordinario", para permitir que "el gobierno controle a los gobernados", pero al mismo tiempo obligar al gobierno a controlarse a sí mismo, es decir, para que las actividades que surgen de estos controles no vaya más allá de las medidas necesarias con respecto a la retención y el acceso a los datos, para no lesionar el derecho de la privacidad de los ciudadanos a priori, garantizando la seguridad al mismo tiempo?[1263]

227. Este es el complejo dilema al que se han enfrentado los tribunales europeos (y nacionales) en los últimos años. Por un lado, la conservación de datos de comunicación permite al "gobierno controlar a los gobernados", proporcionando a las autoridades competentes un medio de investigación que tiene utilidad, aunque con límites, en la lucha contra la delincuencia grave, y en particular en la lucha contra el terrorismo. Por otro lado, no se puede abordar el problema de la necesidad de "obligar al gobierno a controlarse a sí mismo" con respecto al almacenamiento o acceso a los datos conservados, teniendo en cuenta las amenazas al derecho a la privacidad. Por lo tanto, nos encontramos ante la recurrente cuestión de cuál debe ser el "equilibrio entre la protección de la seguridad pública", especialmente con referencia a la necesidad de prevenir ataques terroristas, por una parte, y la protección de privacidad, por otro.

228. El asunto, como sabemos, continúa manifestándose con todas sus implicaciones, especialmente en los últimos años, con la aprobación de una legislación nacional específica de emergencia terrorista, en la afanosa búsqueda de comprender cuál es (y si existe) el nuevo punto de equilibrio entre la privacidad y las razones de orden público y seguridad ciudadana.

229. El TJUE interviene nuevamente en la difícil relación con la obligación de retención general de datos telefónicos y telemáticos, en este caso al decidir sobre sendas leyes estatales que en Suecia y el Reino Unido implementaban la Directiva 2006/24/CE ("*Data Retention*") anulada por el mismo Tribunal con la sentencia *Digital Rights Ireland*, asumiendo este fallo el papel de protagonista absoluto en el camino argumentativo de esta nueva sentencia.

230. Como sabemos, el caso de *Digital Rights Ireland* tuvo un gran impacto en toda la UE[1264], y particularmente en el Reino Unido se prestó mucha atención a la sentencia. Sin

[1263] Esta interesante pregunta, se la plantea Lucia Scaffardi en Lucia SCAFFARDI (2017: 55-56).
[1264] Como ya se demostró ampliamente durante el análisis de las consecuencias que el juicio *Digital Rights Ireland* ha tenido en las leyes y decisiones de los tribunales de los Estados miembros.

embargo, el efecto inmediato de la sentencia estuvo lejos de las expectativas de los defensores de la privacidad, ya que algunos de los Estados miembros de la UE entendieron que la anulación de la Directiva de retención de datos en realidad otorgaba a los Estados una mayor flexibilidad. Hasta ahora, este ámbito estaba co-regulado por la UE y los Estados, pero cuando un elemento de esta corregulación desaparece, quedo discreción del Estado a la luz del principio de subsidiariedad. Sin embargo, esto fue cuestionado por los defensores de la privacidad que todavía consideraban que el artículo 15 de la Directiva sobre la privacidad electrónica de 2002 era la base de la corregulación[1265].

231. A raíz de la sentencia *Digital Rights Ireland* de 2014[1266], se remitieron dos casos al TJUE para evaluar la compatibilidad en Suecia y en el Reino Unido de las leyes nacionales de conservación de datos relativos a las comunicaciones electrónicas, cuya conservación estaba prevista por la Directiva anulada. Por lo tanto, los jueces proporcionan las respuestas necesarias a quienes se preguntaron sobre las consecuencias que tendría esta sentencia sobre las medidas nacionales de transposición de la Directiva o, más en general, sobre la compatibilidad con la legislación de la UE de disposiciones estatales similares a las anauladas en abril de 2014. De hecho, con la sentencia del 21 de diciembre de 2016, *Tele2 Sverige-Watson*, han surgido nuevos indicios sobre este tema, desviando la atención del plan legislativo europeo a la legislación nacional, lo que da como resultado una lectura más exhaustiva del asunto.

232. La sentencia que se va a analizar es relevante para nuestra investigación por el carácter central de la misma en el tema de la seguridad pública en relación con la privacidad, que es de gran relevancia en un momento en que el dominio de las comunicaciones electrónicas sobre la vida privada se enfrenta al necesario control que debe ejercerse para hacer frente a las actividades criminales de dimensión transfronteriza. Esta relevancia explica el surgimiento de mecanismos institucionales que han permitido establecer un

[1265] Artículo 15 (Aplicación de determinadas disposiciones de la Directiva 95/46/CE), apartado 1, de la DIRECTIVA 2002/58/CE: «*Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones* (…)*, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea*».
[1266] Wojciech R. WIEWIÓROWSKI (2017: 177).

estándar común de protección de la privacidad, esto es, un cierto grado de protección de los derechos fundamentales en la legislación europea a través del diálogo constante entre los tribunales y los legisladores.

4.1. El TJUE afirma, otra vez, que la recopilación indiscriminada y la retención de datos de los individuos es ilegal en la Unión Europea

233. La sentencia[1267] tiene su origen en unas cuestiones prejudiciales planteadas en los asuntos acumulados C-203/15 y C-698/15 que se corresponden con la pregunta común sobre si es posible mantener los datos conservados de las comunicaciones en general; datos útiles para enjuiciar delitos, pero que supuestamente se obtienen al actuar fuera de un marco de investigaciones donde la autoridad investigadora solicita a posteriori que controle a ciertos usuarios, por lo tanto, *ex ante* una conservación general de los datos. Por lo tanto, la cuestión consiste en verificar si las herramientas de seguridad pública de retención de datos por parte de las compañías telefónicas, durante un período más prolongado que lo estrictamente necesario, prevalecen sobre los requisitos de privacidad y de qué manera.

234. En Suecia, al día siguiente de la sentencia *Digital Rights Ireland*, el proveedor de servicios de comunicaciones electrónicas establecido en Suecia, *Tele2 Sverige*, notificó a la autoridad sueca de control de los servicios de correos y telecomunicaciones (en adelante, *PTS*) su decisión de dejar de conservar los datos y su propuesta de suprimir los datos ya registrados. Como consecuencia, la Dirección General de la Policía Nacional de Suecia presentó una queja ante la *PTS* porque *Tele2 Sverige* había dejado de comunicarle los datos de los que se trata[1268]. Según la PTS, *Tele2 Sverige* estaba incumpliendo las obligaciones

[1267] Por un atento análisis de la reciente sentencia se vean: Lorna WOODS (2016), «Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)», en *Eu Law Analysis*, 21 December. Disponible en Internet: http://eulawanalysis.blogspot.it/2016/12/data-retention-and-national-law-ecj.html [consulta: 02 de noviembre de 2017]; David ORDÓÑEZ SOLÍS (2017), «Crónica de la jurisprudencia del Tribunal de Justicia de la Unión Europea», en *Cuadernos Europeos de* Deusto, núm. 56, págs. 225-227. Disponible en Internet: http://ced.revistas.deusto.es/article/view/1292 [consulta: 01 de noviembre de 2017]; Valentina FIORILLO (2017), «Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali», en *federalismi.it*, núm. 15, págs. 13 y ss.; Flavio GUELLA (2017), «Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali», en *DPCE on line*, vol. 30, núm. 2, págs. 349-357; Orla LYNSKEY (2017), «Tele2 Sverige Ab and Watson et al: continuity and radical change», en *The European Law Blog*, january 12. Disponible en Internet: http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/ [consulta: 04 de noviembre de 2017]; Oreste POLLICINO y Marco BASSINI (2017).

[1268] En seguida, el Ministro de Justicia designó a un asesor especial para que analizara la normativa sueca controvertida a la luz de la sentencia *Digital Rights Ireland*. El asesor especial llegó a la conclusión de que la normativa nacional relativa a la conservación de datos, tal como estaba establecida en los artículos 16a a 16f de la *LEK*, no era contraria al Derecho de la Unión ni al CEDH. También señaló que la sentencia *Digital Rights Ireland* no podía interpretarse en el sentido de que hubiera censurado el propio principio de la conservación generalizada e indiferenciada de datos.

previstas en la normativa nacional ("*LEK - Lagen om elektronisk kommunikation*")[1269] al no conservar los datos a los que se refiere la *LEK* durante seis meses a efectos de la lucha contra la delincuencia, ordenando, mediante requerimiento, a *Tele2 Sverige* que volviera a conservar esos datos[1270]. El Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, al que se dirige la empresa telefónica después de una sentencia desfavorable en primera instancia, mediante resolución de 29 de abril de 2015, suspendió el procedimiento y presentó las cuestiones prejudiciales al TJUE.

235. Entre tanto, el 17 de julio de 2014, después de tres meses de la anulación de la sentencia *Digital Rights Ireland Ltd*, el gobierno del Reino Unido aprobó la *Data Retention and Investigatory Powers Act 2014* ("*DRIPA*")[1271], medida de emergencia, que prevé periodos variables de conservación de datos hasta 12 meses. El objetivo de la nueva legislación, más política que jurídica, era mantener el *status quo* en lo que respecta a la retención de datos: la nueva ley establecería un sistema muy similar al exigido por la Directiva sobre retención de datos, pero puramente como medida nacional. Era, de hecho, un texto centrado en la posibilidad generalizada de acceso a las comunicaciones de las personas y el uso resultante de los datos obtenidos[1272]. En su nota sobre *Digital Rights Ireland*, el Gobierno del Reino Unido hizo hincapié en que el TJUE sólo analizaba la

[1269] El legislador sueco, a efectos de la transposición de la Directiva 2006/24/CE en el Derecho nacional, modificó la *lagen om elektronisk kommunikation* (Ley sobre comunicaciones electrónicas de 2003) y el *förordningen om elektronisk kommunikation* (Reglamento sobre comunicaciones electrónicas de 2003). Ambas normas, en su versión aplicable al asunto principal, establecen disposiciones sobre la conservación de los datos relativos a las comunicaciones electrónicas y sobre el acceso a esos datos por las autoridades nacionales.

[1270] En contra, *Tele2 Sverige* interpuso un recurso ante el *Förvaltningsrätten i Stockholm* (Tribunal de lo Contencioso-Administrativo de Estocolmo de Suecia). Dicho tribunal desestimó el recurso mediante sentencia de 13 de octubre de 2014. A continuación, *Tele2 Sverige* apeló dicha sentencia ante el órgano jurisdiccional remitente.

[1271] Fue adoptada sólo tres días después en un procedimiento acelerado muy inusual. Vid Niklas VAINIO, Samuli MIETTINEN (2015). Según el primer ministro Cameron, esa medida excepcional era necesaria para proteger las capacidades de intercepción existentes en el temor de que los proveedores de servicios de telecomunicaciones detuvieran la retención y eliminaran los datos. Según el primer ministro británico, las consecuencias de no actuar serían «*grave*». *Vid*. PRIME MINISTER'S OFFICE - Speech, «PM and Deputy PM Speech on Emergency Security Legislation», 11 July 2014. Disponible en Internet: https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation [consulta: 16 de mayo de 2016].

[1272] Los críticos de la ley, sin embargo, señalaban que la "*DRIPA*" no sólo mantiene el *status quo*, sino que también hace que los cambios sustantivos relacionados con la retención de datos no relacionados con las órdenes de interceptación, capacidad de interceptación y acceso a datos de comunicaciones de la ley vigente (Ley de Regulación de Poderes de Investigación) amplíen el alcance de la vigilancia. Si la ley mantiene el *status quo* es difícil de evaluar porque "*DRIPA*" tiene una definición diferente de qué proveedores están obligados a retener los datos. Las nuevas definiciones posiblemente amplían el alcance de la retención. Ahora incluye servicios que consisten en facilitar la creación, gestión o almacenamiento de comunicaciones transmitidas, o que puedan transmitirse, mediante un sistema de telecomunicaciones. Graham SMITH (2014), «Dissecting DRIP - The Emergency Data Retention and Investigatory Powers Bill», en *Cyberleagle*, 12 July. Disponible en Internet: http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html [consulta: 18 de mayo de 2016]; Lucia SCAFFARDI (2017: 68 y ss.).

legalidad de la Directiva de la UE y no las sólidas salvaguardias que ya existen en el régimen de datos de comunicaciones del Reino Unido. El Gobierno afirmaba que el régimen británico ya aborda muchas de las críticas del TJUE y que la nueva ley es igualmente compatible con la doctrina de *Digital Rights Ireland*[1273].

236. Sin embargo, el 17 de julio de 2015, el *UK High Court of Justice* declaró que el artículo 1 ("*Powers for retention of relevant communications data subject to safeguards*") de la "*DRIPA*" era incompatible con la legislación sobre derechos humanos[1274]. El artículo 1 de la "*DRIPA*" establecía que el Ministro del Interior podría exigir mediante notificación ("notificación de conservación") a un operador de telecomunicaciones públicas que conserve datos de comunicaciones relevantes si considera que ello resulta necesario y proporcionado con respecto a uno o varios de los objetivos como, por ejemplo, los intereses de seguridad nacional o, más en general, la seguridad pública o la prevención de un delito. Por lo tanto, se hacía referencia a un catálogo genérico y extremadamente amplio, al cual el Ministro podía adoptar, sin autorización previa de un órgano jurisdiccional o de una entidad administrativa independiente, un régimen general que imponga a los operadores públicos de telecomunicaciones que conserven todos los datos[1275] de comunicaciones durante un período máximo de 12 meses.

237. Mediante sentencia de 17 de julio de 2015, la *High Court of Justice* (*England & Wales*), *Queens' Bench Division* (*Divisional Court*)[1276], declaró que el artículo 1 de la

[1273] Home Office, *Data Retention and Investigatory Powers Act 2014: Further information*, 10 July 2014. Disponible en Internet: https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill [consulta: 18 de mayo de 2016].

[1274] ROYAL COURTS OF JUSTICE, *David Davis and others -v- Secretary of State for the Home Department*, n. EWHC 2092, Case N.: CO/3665/2014, CO/3667/2014, CO/3794/2014, 17 July 2015. Disponible en Internet: https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/ [consulta: 20 de mayo de 2016].

[1275] Aunque dichos datos no incluyen el contenido de las comunicaciones, podrían afectar de modo especial a la vida privada de los usuarios de los servicios de comunicaciones. Lorna WOODS (2016) y Orla LYNSKEY (2017).

[1276] Tribunal Superior de Justicia (Inglaterra y País de Gales) (Sección de lo Contencioso-Administrativo). Los Sres. Peter Brice, Geoffrey Lewis y los parlamentarios ingleses David Davis (conservador) y Tom Watson (laborista), presentaron individualmente ante el Tribunal Superior de Justicia (Inglaterra y País de Gales) (Sección de lo Contencioso-Administrativo), sendos recursos contencioso-administrativos por los que solicitaban el control de la legalidad del artículo 1 de la "*DRIPA*", invocando en particular la incompatibilidad de dicho artículo con los artículos 7 y 8 de la Carta y con el artículo 8 del CEDH. Alan TRAVIS (2014), «Drip Surveillance Law Faces Legal Challenge by MPs», en *The Guardian*, 22 July. Disponible en Internet: http://www.theguardian.com/world/2014/jul/22/drip-surveillance-law-legal-challenge-civil-liberties-campaigners [consulta: 18 de mayo de 2016]; «Press Release: Permission Granted for Judicial Review of DRIPA», en *Open Rights Group*, December 08, 2014. Disponible en Internet: https://www.openrightsgroup.org/press/releases/press-release:-permission-granted-for-judicial-review-of-ripa [consulta: 18 de mayo de 2016]. En particular, el político británico David Davis ha presentado al TJUE la cuestión de la legitimidad de las interceptaciones masivas del *GCHQ* del Reino Unido (la agencia de seguridad

"*DRIPA*" no era compatible con los artículos 7 y 8 de la Carta, puesto que no establece normas claras y precisas en relación con el acceso y la utilización de esos datos conservados y no supedita el acceso a dichos datos a un control previo llevado a cabo por un órgano jurisdiccional o por una entidad administrativa independiente. Según dicho órgano jurisdiccional la sentencia *Digital Rights Ireland* enunciaba «*requisitos imperativos de Derecho de la Unión*» aplicables a las normativas de los Estados miembros en materia de conservación de datos de comunicaciones, así como de acceso a dichos datos. Por lo tanto, puesto que el TJUE, en la citada sentencia, había estimado que la Directiva 2006/24/CE era incompatible con el principio de proporcionalidad, una normativa nacional que tuviera un contenido idéntico al de dicha Directiva tampoco podía ser compatible con ese principio[1277]. Como sabemos, una normativa que establece un régimen generalizado de conservación de datos de comunicaciones vulnera los derechos garantizados en los artículos 7 y 8 de la CDFUE, salvo que esa normativa se complete con un régimen de acceso a los datos, definido por el Derecho nacional, que prevea suficientes garantías para la salvaguarda de esos derechos.

238. Tras la resolución que consideró la regulación nacional incompatible con esos artículos, el gobierno de Theresa May apeló esa decisión, siendo el *Court of Appeal* (*England & Wales*) (*Civil Division*) el que planteó las cuestiones prejudiciales.

239. Si bien los dos casos parecen ser coincidentes, debe especificarse que la senda petición de decisión prejudicial planteada por el Tribunal de Apelación de lo Contencioso-

que se ocupa de interceptaciones y espionaje). La nueva normativa británica "*Investigatory Powers Bill 2016*" (llamada por los críticos "*The snoopers' charter*") entró en vigor con el nuevo año (reemplazada la anterior porque era contraria a la legislación europea por el Tribunal Superior de Justicia británico) y parece ser una de las más invasiva y exigentes, imponiendo a los proveedores recoger y también conservar los datos de navegación de los usuarios durante 12 meses, lo que obviamente permite a las autoridades un amplio acceso a dichos datos. *Vid*. Owen BOWCOTT (2016), «MP calls for limit on UK surveillance powers as EU test case opens», en *The Guardian*, 12 April. Disponible en Internet: https://www.theguardian.com/world/2016/apr/12/mp-david-davis-calls-limit-uk-surveillance-powers-european-court-justice; Alan TRAVIS (2016), «'Snooper's charter' bill becomes law, extending UK state surveillance», en *The Guardian*, 29 November. Disponible en Internet: https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance [consulta: 03 de noviembre de 2017]; «Il Regno Unito verso la sorveglianza totale: "Un attacco alla democrazia"», en *Valigia Blu*, 3 de diciembre 2016. Disponible en Internet: http://www.valigiablu.it/uk-legge-sorveglianza/. Sobre la legislación británica, *vid*. «Investigatory Powers Bill: Commons stages», en *Parliament.uk*, 30 November 2016. Disponible en Internet: http://www.parliament.uk/business/news/2016/march/investigatory-powers-bill-commons-second-reading/ [documentos consultados: 03 de noviembre de 2017]

[1277] Parece que la *High Court*, en continuidad con el pronunciamiento de los jueces de Luxemburgo, había promulgado una serie de indicaciones mediante las cuales era posible desarrollar una actividad masiva de recopilación de datos, sujeta a ciertas condiciones, para proteger a las personas de un uso impropio de la información, con una posible violación del derecho a la privacidad.

Administrativo de Estocolmo (asunto C-203/15) es más compleja[1278], ya que también se refiere a un parámetro interpuesto, como ya ocurrió por la Directiva 95/46/CE en el caso *Digital Rights Ireland*. Por lo tanto, la primera pregunta del caso *Tele2 Sverige-Watson* ocupa la mayor parte del razonamiento del TJUE, y, en síntesis, es la siguiente: una obligación general de conservar datos de tráfico y localización sin ninguna distinción, limitación o excepción en función del objetivo «*¿es compatible con el artículo 15, apartado 1, de la Directiva 2002/58/CE, habida cuenta de los artículos 7, 8 y 52, apartado 1, de la Carta?*»

240. En segundo lugar, el TJUE resuelve la segunda cuestión del caso *Tele2 Sverige-Watson* y la primera del caso británico (asunto C-698/15)[1279], condensándola como la pregunta de si el artículo 15, apartado 1, de la misma Directiva se opone al acceso sin limitación por parte de autoridades nacionales a datos de tráfico y localización en el marco de la lucha contra la delincuencia.

241. A la luz de las cuestiones planteadas al TJUE[1280], el fallo parece ser sintomático de una "incertidumbre generalizada"[1281] sobre las implicaciones reales de la decisión de *Digital Rights Ireland* y la consiguiente anulación de la Directiva sobre conservación de datos con respecto a medidas formalmente fuera del ámbito de aplicación de la Directiva misma y su transposición en la legislación nacional.

242. Las peticiones de decisión prejudicial tienen por objeto la interpretación del artículo 15, apartado 1, de la «*Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la*

[1278] Valentina FIORILLO (2017).
[1279] TJUE (Gran Sala), *Tele2 Sverige AB y Post- och telestyrelsen, y Secretary of State for the Home Department y Tom Watson, Peter Brice, Geoffrey Lewis*, asuntos acumulados C-203/15 y C-698/15, sentencia de 21 de diciembre de 2016, apartado 59. De forma aún más explícita y directa, y sin referencia a las normas de la legislación de la UE, el Tribunal de Apelaciones de Inglaterra y Gales (*Court of Appeal*) ha decidido suspender el procedimiento y plantear al TJUE las siguientes cuestiones prejudiciales: 1) si la sentencia *Digital Rights Ireland* (en particular sus apartados 60 a 62) establece «*requisitos imperativos de Derecho de la Unión que resulten aplicables al régimen nacional de un Estado miembro que regula el acceso a los datos conservados de conformidad con la legislación nacional, al objeto de dar cumplimiento a los artículos 7 y 8 de la Carta*»; y 2) si la sentencia *Digital Rights Ireland* «*amplía* (…) *el alcance de los artículos 7 u 8 de la Carta más allá del alcance del artículo 8 del CEDH*», como se establece en la jurisprudencia del TEDH.
[1280] El TJUE, ordenó la acumulación de los asuntos C-203/15 y C-698/15 a efectos de la fase oral y de la sentencia, de los procedimientos prejudiciales, con arreglo al artículo 267 del TFUE, por el Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo (*Kammarrätten i Stockholm*) y el Tribunal de Apelación (Inglaterra y País de Gales) (Sección de lo Civil) (*Court of Appeal*) (*England & Wales*) (*Civil Division*).
[1281] Oreste POLLICINO y Marco BASSINI (2017: 5).

intimidad en el sector de las comunicaciones electrónicas» (Directiva sobre la privacidad y las comunicaciones electrónicas, dicha también "Directiva *e-Privacy*")[1282]. El artículo 15, apartado 1, de la Directiva de 2002, que hace referencia a una disposición similar ya incluida en la Directiva 95/46/CE, establece un tipo de cláusula de salvaguardia para la autonomía del Estado. En particular, el artículo 15 de la mencionada Directiva, con el epígrafe "Aplicación de determinadas disposiciones de la Directiva" (se refiere a la Directiva 95/46/CE), enuncia: que «*los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones*» a la protección de datos personales, cuando tal limitación constituya «*una medida necesaria, proporcionada y apropiada en una*

[1282] La Directiva fue adoptada en 2002 para abordar todos los riesgos que los numerosos y ampliamente difundidos servicios de comunicaciones electrónicas representan para el procesamiento automatizado de datos de suscriptores y usuarios. Esta Directiva ha sido modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, y actualmente es objeto de un importante proceso de revisión en el marco del procedimiento legislativo ordinario. En enero de 2017, la Comisión presentó una PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM (2017) 10 final, 2017/0003(COD), Bruselas, 10.1.2017. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0010 [consulta: 18 de mayo de 2017]. Cabe destacar que esta propuesta pretende actualizar, a la luz de los últimos avances tecnológicos, las normas de privacidad en el campo de las comunicaciones electrónicas para garantizar, por un lado, un mayor nivel de protección de la privacidad, armonizado en toda la Unión Europea y, por otro, nuevas oportunidades para la innovación empresarial. *Vid*. Carlos B. FERNÁNDEZ (2017a), «¿Qué enmiendas deben introducirse en la propuesta de Reglamento europeo sobre ePrivacidad?», en *Diario La Ley*, 2-6-2017; y del mismo autor, «El Parlamento Europeo avanza en la tramitación del Reglamento de E-Privacy con las primeras propuestas de modificación», en *Diario La Ley*, 14-6-2017. Además, el objetivo de la propuesta es crear un sistema normativo sólido y actualizado, de conformidad con el reciente RGPD. En este sentido, Paula ORTIZ LÓPEZ (2017), «Regulando la privacidad del futuro. Análisis de la Propuesta de Reglamento europeo de e-Privacy y su interconexión con el Reglamento General de Protección de Datos», en *Diario La Ley*, núm. 10, Sección Ciberderecho, 4 de octubre de 2017. Antes de esta propuosta de reforma, faltaba una norma común de protección de la privacidad en el campo de datos de las comunicaciones electrónicas y la ausencia inicial, si entran en juego cuestiones de seguridad pública, de armonizar la materia en la Unión Europea. La ausencia de una norma común no encontró parámetros precisos incluso en la jurisprudencia del Tribunal de Estrasburgo, que, al aplicar el artículo 8 del CEDH, ha mantenido la protección en niveles necesariamente flexibles, posponiéndose de vez en cuando el control de proporcionalidad. En este sentido, el TEDH no impone una prohibición absoluta, aunque reconoce, sobre la base del artículo 8, que el acceso de las autoridades nacionales competentes a los datos es una interferencia (*vid*. sentencias TEDH, *Leander contra Suecia*, apartado 48 y *Rotaru contra Romania*, apartado 46). Por lo tanto, deben introducirse «*reglas claras y precisas*» que disciplinen «*el alcance y la aplicación*» de la medida invasiva, incluidos los requisitos mínimos para que las personas cuyos datos han sido almacenados tengan garantías contra el riesgo de abuso, excesos y uso indebido de datos (*vid*. TEDH, *Rotaru contra Romania*, apartados 57 a 59). En particular, con mayor atención cuando los datos personales están sujetos a un procesamiento automático y, por lo tanto, a la recopilación general de datos de tráfico telefónico, sin que la recopilación generalizada esté necesariamente prohibida (*vid*. TEDH, *S. and Marper contra Reino Unido*, apartado 102). Por lo tanto, la Unión Europea es libre de establecer reglas que permitan la retención y el acceso a datos confidenciales, posiblemente incluso con modalidad automática y masiva, pero dictando unas garantías procesales que el TEDH requiere como estándar mínimo de tutela de la vida privada. Por otro lado, la Unión Europea también es libre de establecer un nivel de protección más elevado, reduciendo el procesamiento *ex ante* de datos de forma más drástica, que se mantendrá para fines no actuales de protección de la seguridad pública (como exige el artículo 52, apartado 3, de la CDFUE). Flavio GUELLA (2017). También, véase EDPS (2017b), EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 24 April 2017, págs. 40. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf [consulta: 26 de julio de 2017].

sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva [95/46]»[1283]. Con este fin, los Estados miembros pueden adoptar, además, medidas legislativas que permitan que los datos se almacenen durante un período de tiempo limitado.

243. Mediante la sentencia *Tele2 Sverige-Watson* se lleva a cabo una reducción de los espacios de estas excepciones a la protección de los datos personales previstas del artículo 15, apartado 1, al exigir que se consideren conforme a su naturaleza, esto es, de manera excepcional. Esta es una interpretación restrictiva del artículo 15, apartado 1, primera frase, de la Directiva 2002/58/CE que establece unos objetivos de carácter exhaustivo[1284] – deben tener como finalidad «*proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas*», o deben perseguir alguno de los demás objetivos considerados en el artículo 13, apartado 1, de la Directiva 95/46/CE – de tal forma que los Estados no podrán aducir razones especiales con respecto a la seguridad pública para restringir razonablemente la protección de los derechos fundamentales garantizados por la CDFUE, pero, sobre todo, se argumenta que es necesario equilibrar estos derechos con los niveles de protección y las disposiciones operativas proporcionales ahora descritos por el propio TJUE[1285]. Estos objetivos que pueden justificar una normativa nacional que establezca una excepción al principio de confidencialidad, debe guardar «*una relación con la gravedad de la injerencia en los derechos fundamentales*» que supone este acceso, de ello se deriva que sólo la lucha contra la delincuencia grave puede justificar dicho acceso a los datos conservados[1286].

244. El respeto del principio de proporcionalidad se desprende igualmente de la reiterada jurisprudencia del TJUE[1287] según la cual la protección del derecho fundamental al respeto de la vida privada de la UE requiere «*que las excepciones a la protección de los datos*

[1283] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 11.
[1284] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 90. *Vid*. Lorna WOODS (2016) y Orla LYNSKEY (2017).
[1285] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 91. Véanse, por analogía, por lo que se refiere a la Directiva 95/46, las sentencias del TJUE, *Österreichischer Rundfunk y otros*, apartado 68; *Google Spain*, apartado 68, y, *Schrems*, apartado 38.
[1286] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 115.
[1287] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 52; y *Schrems contra Data Protection Commissioner*, apartado 92.

personales y las limitaciones de esa protección no excedan de lo estrictamente necesario»[1288]. El punto de partida, por lo tanto, es considerar las características de las operaciones de tratamiento de datos autorizados por la Directiva. En este sentido, el Tribunal declara claramente que la normativa sueca «*prevé una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica, y obliga a los proveedores de servicios de comunicaciones electrónicas a conservar esos datos de manera sistemática y continuada, sin ninguna excepción*». Por lo tanto, hay coincidencia entre las categorías de datos procesados en virtud de la Directiva 2006/24/CE anulada y los de la legislación sueca[1289].

245. La sentencia, con el fin de definir esta proporcionalidad, reproduce a continuación los fundamentos de la sentencia *Digital Rights Ireland* de 2014[1290], admitiendo que, dentro de los límites del respeto derechos fundamentales, sólo la lucha contra la delincuencia grave puede justificar una medida excepcional de este tipo. Por lo tanto, sólo se puede considerar que no infringen la legislación de la UE las normas nacionales que proporcionan «*una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia*»[1291].

246. Bajo este planteamiento, el Tribunal continúa aplicando los mismos estándares que ya se han utilizado en *Digital Rights Ireland*. Una conservación de los datos de tráfico generalizada, sin «*ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr*», incluso afecta globalmente a todas las personas que hacen uso de servicios de comunicaciones electrónicas, aunque no se encuentren, «*ni siquiera indirectamente, en una situación que justifique una acción penal,* (…) *se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves*»[1292] es una normativa nacional que excede, por tanto, los límites de lo estrictamente necesario y no

[1288] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 96.
[1289] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 97. Lorna WOODS (2016).
[1290] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 60 y 59.
[1291] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 106. *Vid*. Orla LYNSKEY (2017).
[1292] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartados 105 y 107.

puede considerarse justificada en una sociedad democrática[1293], como exige el artículo 15, apartado 1, de la Directiva 2002/58/CE, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la CDFUE[1294].

247. La normativa sueca en cuestión obliga a los prestadores de servicios de telecomunicaciones a recopilar todos los datos de tráfico y localización sin establecer un filtro o limitación alguna, amparándose en el «*objetivo de la lucha contra la delincuencia*». El conjunto de estos datos permite «*extraer conclusiones muy precisas sobre la vida privada de las personas*», todo ello sin conocimiento o autorización de los usuarios[1295]. Así, al no existir relación alguna entre los datos cuya conservación se establece y los objetivos que pretenden perseguirse, se considera esta normativa nacional contraria a la Directiva, puesto que convierte en regla general la excepción.

248. Siguiendo su razonamiento, el TJUE enumera los requisitos que debe tener una normativa nacional para permitir el acceso a esos datos a autoridades nacionales.

249. El criterio de proporcionalidad establecido en la sentencia *Digital Rights Ireland* se aplica a la discrecionalidad estatal, no sólo a los principales argumentos relativos a la conservación de datos sino también al acceso por parte de las autoridades nacionales competentes. El TJUE señala que una normativa nacional que reconozca un acceso general a los datos conservados no puede considerarse limitado a lo estrictamente necesario. La normativa debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos de los abonados o usuarios registrados. Consecuentemente, sólo podrá concederse un acceso en relación con el objetivo de la lucha contra la delincuencia a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave[1296]. A este respecto el

[1293] El SEPD adopta un enfoque similar al evaluar la necesidad de medidas que limiten el derecho fundamental a la protección de datos personales en su "Kit de herramientas de necesidad" ("*Necessity Toolkit*"). El "Kit" de herramientas tiene como objetivo ayudar a la evaluación del cumplimiento de las medidas propuestas con la legislación de la UE sobre protección de datos. Fue desarrollado para equipar mejor a los legisladores y legisladores de la UE responsables de preparar o examinar las medidas que implican el tratamiento de datos personales y limitar el derecho a la protección de datos personales y otros derechos y libertades establecidos en la Carta. EDPS (2017a), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, Brussels, 11 April 2017, págs. 29.
[1294] «Los proveedores de servicios de comunicaciones no están obligados a una conservación general de datos de sus usuarios», en *Diario La Ley*, 21-12-2016.
[1295] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 99.
[1296] Véase, por analogía, TEDH, *Roman Zakharov contra Rusia*, apartado 260.

TJUE aclara que, en "situaciones particulares", como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública, podría igualmente concederse el acceso a los datos de otras personas cuando «*existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades*»[1297]. Por lo tanto, se infringe la legislación de la UE en la normativa nacional que no limita dicho acceso únicamente al objetivo de luchar un delito grave o que no permite el acceso a «*un control previo por un órgano jurisdiccional o de una entidad administrativa independiente*»[1298].

250. En esta sentencia, así como en *Digital Rights Ireland*, el TJUE parte de la consideración obvia de que el acceso a los datos de las comunicaciones electrónicas permite deducir "conclusiones muy precisas sobre la privacidad de las personas", la interferencia con los derechos de los ciudadanos debido a dicho acceso debe, por lo tanto, considerarse como extremadamente grave y afectar la vida de las personas, y también al limitar seriamente el ejercicio de los derechos fundamentales[1299].

4.2. Lucha contra el crimen y la privacidad: ¿la seguridad de un país justifica la violación "masiva" de la privacidad de los ciudadanos?

251. De todo lo anterior puede comprobarse como la sentencia *Tele2 Sverige*-Watson resulta de gran importancia, no ya por la innovación de los principios de la sentencia, sino porque con esta sentencia el TJUE completa un ciclo – a través del diálogo con algunos Tribunales Constitucionales nacionales en los últimos años[1300] – que ha llevado un innegable grado de protección que se impone uniformemente a todos los Estados miembros, limitando su autonomía legislativa a través de los principios de necesidad y proporcionalidad, que en *Digital Rights Ireland*, sin embargo, sólo vinculaban el legislador europeo. Sin embargo, las

[1297] TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartado 119. Valentina FIORILLO (2017).
[1298] Por analogía, véase, respecto a la Directiva 2006/24/CE, la sentencia *Digital Rights Ireland Ltd y otros*, apartado 62. *Vid*. igualmente, por analogía, en relación con el artículo 8 del CEDH, TEDH, *Szabó and Vissy contra Hungría*, apartados 77 y 80. TJUE (Gran Sala), *Tele2 Sverige-Watson*, apartados 120 y 125. Lorna WOODS (2016).
[1299] El hecho de que los datos se recopilen y almacenen sin siquiera informar al ciudadano puede llevarlo a creer que está bajo vigilancia constante con todas las implicaciones obvias para la vida privada. Implicaciones analizadas en un estudio alemán hace unos años y uno por el periódico *The Washington Post*: Rick FALKVINGE (2016), «German studies eight years ago show that surveillance brings horrible self-censorship. Why is this news to the US now?», en *privateinternetaccess.com*, Mar 30. Disponible en Internet: https://www.privateinternetaccess.com/blog/2016/03/germans-studies-eight-years-ago-show-surveillance-brings-horrible-self-censorship-news-us-now/; Karen TURNER (2016), «Mass surveillance silences minority opinions, according to study», en *The Washington Post*, March 28. Disponible en Internet: https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.2f592e5d7ace [documentos consultados: 27 de octubre de 2017].
[1300] En ese sentido, véase el apartado sobre la sentencia *Digital Rights Ireland*.

fuertes y marcadas afinidades con los principios trazados en la *Digital Rights Ireland* representan la noticia más relevante y destacada. Los jueces de Luxemburgo no sólo confirman el alcance interpretativo de los artículos 7 y 8 de la CDFUE, sino que subrayan una relación importante entre estas disposiciones de derecho originario y los actos de legislación secundaria, tanto que, en ambas sentencias de retención de datos reemplazan las normas interpuestas como Directiva 95/46/CE y la Directiva 2002/58/CE. De hecho, en el juicio en *Tele2 Sverige-Watson*, es evidente que el artículo 15, apartado 1, de la Directiva sobre privacidad electrónica debe interpretarse a la luz de la Carta en el sentido de que se opone a una normativa nacional que presenta una interferencia masiva en el derecho a la protección de los datos personales de los ciudadanos[1301].

252. En esta sentencia, las disposiciones de protección de la privacidad se utilizan para reafirmar la prevalencia de la protección de datos sobre las instancias estatales de seguridad, invalidando la ley estatal, con el efecto indirecto de reafirmar el papel central del TJUE en su rol guardián de la Carta y la aplicación inequívoca y uniforme de la legislación de la UE en todos los Estados miembros[1302]. La respuesta del Tribunal no deja lugar a ambigüedades: la seguridad de un país no justifica la violación "masiva" de la privacidad de los ciudadanos[1303].

253. El margen de maniobra que la Directiva reconoce a los Estados miembros, mediante la integración de una excepción al régimen ordinario de protección de la privacidad, debe

[1301] Javier FERNÁNDEZ-LASQUETTY y Martín BELLO (2017), «La legislación europea no permite una normativa nacional que recopile datos de tráfico y localización de manera indiscriminada. Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, Tele2 Sverige (C-203/15 y C-698/15)», en *Anuario ELZABURU de jurisprudencia europea en propiedad industrial e intelectual*, págs. 139-141. Disponible en Internet: http://www.elzaburu.es/en/document-centre/search-news-items?op=viewcms&id2=-3005116 [consulta: 03 de noviembre de 2017].

[1302] En Lorna WOODS (2016). La decisión parece puramente académica para el Reino Unido, ya que con el *Brexit* ya no estará sometido a la jurisdicción de las instituciones europeas. Pero, de hecho, los británicos tendrán que lidiar con esa decisión, lo que afectará los flujos transfronterizos de datos. En concreto, los puntos de referencia del TJUE deberán evaluarse cuando se verifique la "adecuación" de la legislación de un país para autorizar la transferencia de datos de ciudadanos europeos por parte de las empresas de ese país, con el riesgo de que muchas empresas podrán decidir cambiar legislación con un Estado que cumpla con la legislación comunitaria. Por el contrario, otros países europeos no podrán ignorarlo, especialmente en un período histórico en el que varios Estados están introduciendo enmiendas legislativas a una recopilación cada vez más amplia de datos de ciudadanos para luchar contra el terrorismo. Vid. Bruno SAETTA (2016d), «La Corte europea dice che la sorveglianza di massa è illegittima. Di nuovo», en *Valigia Blu*, 27 diciembre. Disponible en Internet: http://www.valigiablu.it/corte-europea-sorveglianza-massa/ [consulta: 02 de noviembre de 2017]; Orla LYNSKEY (2017).

[1303] La sentencia asesta un golpe a la nueva ley británica sobre antiterrorismo, la *Investigatory Powers Act 2016*, promovida por la primera ministra Theresa May, destinada a otorgar más poderes de control a las autoridades británicas sobre los correos electrónicos, sino también en el seguimiento de la navegación de Internet del ciudadano. Según el dictamen de la Corte, esta práctica viola los límites de toda sociedad democrática. Vid. ampliamente, Alan TRAVIS (2016).

interpretarse de forma restrictiva. En este sentido, el TJUE permite la posibilidad de que los Estados impongan obligaciones de recopilación de datos para fines específicos únicamente con el objeto de la represión o el combate de delitos graves, siempre que estén limitados temporalmente y a los datos estrictamente necesarios. Además, el acceso a los datos por parte de las autoridades debería estar sujeto a condiciones específicas, incluido el control por una autoridad independiente (tribunal o entidad pública) y los datos deben mantenerse dentro del territorio de la Unión.

254. También, en este caso, frente a sendas peticiones de decisión prejudicial como las presentadas por los tribunales sueco e inglés, debe señalarse de inmediato que, aunque no se apartó del nivel formal, el TJUE ha argumentado y ha desarrollado un tipo de pronunciamiento que adquiere la sustancia (pero no la forma) de una "declaración de nulidad"[1304], evidentemente análoga a *Digital Rights Ireland* y similar a lo que ya sucedió en *Schrems*.

255. Para concluir, la sentencia comentada basa el estándar de privacidad en la interpretación de Directiva, lo que permite la evaluación pacífica como el Derecho de la Unión no admite una conservación generalizada e indiferenciada de los datos[1305]. En concreto, el artículo 15, apartado 1, de la Directiva 200/58/CE (transpuesto al artículo 11 del nuevo RGPD) interpretado en relación con los artículos 7 y 8 de la CDFUE, lleva a la conclusión de que una normativa nacional que, con el fin de combatir la delincuencia, permite una recopilación indiscriminada de datos de ciudadanos es incompatible con la legislación comunitaria.

256. En definitiva, si bien puede observarse cómo las nuevas tecnologías aplicadas a las investigaciones son una herramienta útil para combatir el crimen en general y el terrorismo en particular, el impacto de estas técnicas en las condiciones del individuo requiere una evaluación cuidadosa, en tanto pueden comportar fuertes limitaciones a los derechos individuales. En este sentido, resulta un elemento esencial la individualización de la recopilación de datos, ya que la vigilancia nunca puede generalizarse, pues debe necesariamente identificar las personas sospechosas, o una serie de premisas supuestamente involucradas en delitos. Además, deben recordarse los criterios objetivos que deben

[1304] Observación por Valentina FIORILLO (2017: 17).
[1305] Orla LYNSKEY (2017).

cumplirse, que deben establecer un vínculo entre el objetivo perseguido y los datos que deben conservarse.

257. Finalmente, la sentencia es un paso más en la limitación de la injerencia de autoridades estatales en la vida privada de los individuos, continuando la línea de las sentencias *Schrems* y *Digital Rights Ireland*. Además, considera los datos de localización y tráfico, en su conjunto, como datos personales, ya que permiten trazar un perfil muy preciso de la persona afectada, llegando casi a la vigilancia continua[1306].

258. Si bien la sentencia estaba dirigida a las normas estatales de los Estados implicados en el asunto, su contenido tendrá seguro un importante impacto en las medidas antiterroristas adoptadas por los gobiernos europeos que afrontan amenazas de ataques territorias como los de Madrid, París, Bruselas, Berlín o Barcelona. Por lo tanto, la sentencia se dicta en un momento en el que los atentados aumentan el poder otorgado por los gobiernos a las instituciones de seguridad que ven obstaculizadas sus estrategias por aquellos partidarios de la privacidad que defienden que la conservación de datos "salvaje", no sólo es contraria a los derechos fundamentales de los ciudadanos, sino que además es ineficaz en la lucha contra el terrorismo.

[1306] Javier FERNÁNDEZ-LASQUETTY y Martín BELLO (2017).

CAPÍTULO V

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LA DIRECTIVA DE PROTECCIÓN DE DATOS EN LOS SECTORES POLICIAL Y JUDICIAL. LOS NUEVOS LÍMITES DE ESTADO A LA LIBERTAD EN EUROPA

1. Una aproximación a la evolución del sistema de protección de datos en la UE

1. En la Unión Europa, como es bien sabido, el actual conjunto de normas en materia de privacidad es el resultado de un proceso normativo que se inició a mediados de los años noventa, con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que definió, por primera vez, un marco normativo con el fin de establecer un equilibrio entre un alto nivel de protección de la privacidad de las personas y la libre circulación de los datos personal en la UE. Tras su adopción, la UE ha regulado una serie de cuestiones importantes con respecto a la protección de datos[1307], incluyendo, en relación con el objeto de nuestro análisis, la protección de datos personales tratados en el marco de la policía y la cooperación judicial en materia penal, así como el tratamiento y la transferencia de datos personales a terceros países. A pesar de que se ha asistido a un proceso de fortalecimiento del nivel de protección de la vida privada con la entrada en vigor del Tratado de Lisboa (artículo 16 del TFUE), aún persiste mucha problemática en la aplicación de los derechos garantizados por la legislación europea a la luz de algunas supuestas contradicciones.

2. La armonización de los sistemas jurídicos de los Estados miembros, con respecto a la cuestión de la privacidad, se hace necesaria también por los numerosos y frecuentes

[1307] Entre éstas, se puede también incluir: el Reglamento (CE) n. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, ahora derogado por el nuevo Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos; la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) y la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Debe recordarse que, con la sentencia de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland* y *Seitlinger y otros*, el TJUE anuló la Directiva 2006/24/CE.

pronunciamientos judiciales de los últimos años, por parte del TEDH[1308], TJUE y de los Tribunales Constitucionales nacionales; además de la constante actividad consultiva por el Grupo de Trabajo[1309], y por el SEPD[1310].

3. En este escenario caracterizado por la incertidumbre en términos de regulación en la Unión Europea –que se ha puesto de manifiesto en los capítulos anteriores–, tras quince años desde la primera Directiva relativa a la protección de datos personales y libre circulación de los mismos, y ante la imposibilidad de lograr el objetivo de establecer un marco jurídico uniforme en toda Europa[1311] y ante los importantes cambios tecnológicos[1312], las

[1308] Se trata de dos sentencias del TEDH analizadas anteriormente, que proporcionan todos los elementos para una evaluación de los programas gestionados de acuerdo con los métodos tradicionales de la *NSA*, y por tanto también del programa *TEMPORA* proporcionado por el Reino Unido. Se trata de las sentencias: *Roman Zakharov contra Rusia*, núm. 47143/06, de 4 de diciembre de 2015, con el que Rusia ha sido condenada por el poder reconocido a los servicios secretos y la policía para llevar a cabo la vigilancia y las escuchas telefónicas de los dispositivos móviles de una manera arbitraria y abusiva; y sobre todo de la sentencia *Szabó y Vissy contra Hungría*, núm. 37138/14, de 12 de enero de 2016, con la que Hungría también ha sido condenada por las escuchas telefónicas y telemáticas por los servicios de inteligencia, hechas posibles por una ley antiterrorista de 2011. En las sentencias ahora mencionadas, el TEDH establece que los dos gobiernos han violado el derecho al respeto de la vida privada y la correspondencia, como exige el artículo 8 del CEDH. En otras palabras, con referencia al tratamiento de los datos personales, el Tribunal de Estrasburgo muestra cómo, incluso en la legítima necesidad de reforzar la seguridad y la prevención, siempre debe tenerse debidamente en cuenta los principios de necesidad, finalidad, proporcionalidad y temporalidad.

[1309] El Grupo de Trabajo, en este sentido, ha emitido y realizado diversos dictámenes con aportaciones útiles. En particular, con carácter meramente ejemplificativo y no exhaustivo véase: ARTICLE 29 DATA PROTECTION WORKING PARTY - Working Party on Police and Justice (2009); GRUPO DE PROTECCIÓN DE DATOS DEL ARTICULO 29 (2010), Dictamen 8/2010 sobre el Derecho aplicable, 0836-02/10/ES, WP 179, emitido el 16 de diciembre de 2010, págs. 39. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf [consulta: 29 de enero de 2017]; ARTICLE 29 DATA PROTECTION WORKING PARTY (2011a).

[1310] El SEPD también emitió dictámenes y opiniones sobre los temas planteados. Con carácter meramente ejemplificativo y no exhaustivo vid.: SEPD (2011); EDPS (2013), Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, Brussels, 14 June 2013, págs. 9 y ss.

[1311] El instrumento de la directiva, de hecho, requiere la aplicación de los legisladores nacionales en los distintos Estados miembros, que deben adaptar sus legislaciones a la directiva misma, con un cierto margen de apreciación en cuanto a la especificación de su contenido, imponiendo a la directiva solamente una obligación de resultado.

[1312] En la misma línea, la Comisión Europea ha declarado en varias ocasiones que el desarrollo de la economía digital en la Unión Europea en los últimos años ha sido de forma menos rápida y eficiente que la evolución experimentada en los EE.UU., con la pérdida competitiva de los operadores europeos. Incluso la financiación europea, en la innovación y la investigación en el campo de las tecnologías digitales, han demostrado que las actividades hasta hoy en este campo se encuentran mal coordinadas. *Cfr*. EUROPEAN COMMISSION (2014), Communication on data-driven economy, Brussels, 02/07/2014. Disponible en Internet: http://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy [consulta: 02 de febrero de 2017]; EUROPEAN COMMISSION - Fact Sheet (2015a), Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, Brussels, 28 January 2015. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm [consulta: 02 de febrero de 2017]; COMISIÓN EUROPEA - Comunicado de prensa (2015a), Apoyo de los ministros de Justicia a la propuesta de la Comisión de fijar nuevas normas de protección de datos para impulsar el mercado único digital de la UE, Luxemburgo, 15 junio 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-5176_es.htm [consulta: 02 de febrero de 2017].

instituciones europeas comenzaron pensar en nuevos instrumentos[1313], como un reglamento y una directiva, que permitiesen una verdadera armonización de las normas sobre la privacidad en los sistemas jurídicos de los Estados miembros.

4. Por consiguiente, la necesidad de establecer unos criterios más adecuados y estables en el tratamiento de datos personales ha sido una de las principales razones que impulsaron a la Comisión Europea a llevar a cabo la revisión de la Directiva 95/46/CE, iniciándose así una reforma integral de todo el régimen jurídico de los datos personales en todas sus dimensiones, incluida en lo que afecta a la cooperación en asuntos de justicia y de interior (seguridad y orden público)[1314]. Precisamente sobre este último punto, el Parlamento Europeo se ha interrogado en los últimos años, planteando la problemática de la protección de datos en el ELSJ con el objetivo de aplicar los principios contenidos en la Directiva 95/46/CE, también al ámbito de la cooperación judicial y policíal, abriendo así un frente para encontrar un equilibrio entre las exigencias de la lucha contra la delincuencia y el respeto a la privacidad[1315].

5. En el año 2010 el Consejo Europeo invitó a la Comisión Europea a «*evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas*» y no legislativas[1316].

[1313] *Amplius*, *vid*. Serge GUTWIRTH, Ronald LEENES, Paul DE HERT (eds.) (2015), *Reforming European Data Protection Law*, Dordrecht, Springer Netherlands, págs. 406. ISSN: 2352-1929.

[1314] El Programa de Estocolmo fue la primera iniciativa post-Lisboa que determinó la nueva legislación en el ámbito del ELSJ, incluyendo el tratamiento de la información con finalidades de seguridad. La legislación uniforme de la UE permite una cooperación efectiva entre las autoridades públicas. Sin embargo, el Programa de La Haya de 2005 estableció prioridades para el Área de Libertad, Seguridad y Justicia, y describió el principio de disponibilidad como la posibilidad de que la autoridad pública de un Estado miembro obtenga información de otro Estado miembro. Por lo tanto, se incluía el intercambio de información como uno de los objetivos clave en los siguientes cinco años. También preveía el incremento de recogida e intercambio de información con el objetivo de gestionar los desplazamientos migratorios, así como controlar y prevenir delitos. Véase EL PROGRAMA DE LA HAYA: CONSOLIDACIÓN DE LA LIBERTAD, LA SEGURIDAD Y LA JUSTICIA EN LA UNIÓN EUROPEA, *supra*.

[1315] Entre los casos de estudios de la investigación del Parlamento, se incluye el uso de escáneres corporales ("*body scanners*") considerado la nueva frontera para la lucha contra el terrorismo, que no puede prevalecer sobre el derecho a la protección de datos. *Vid*. Didier BIGO, Sergio CARRERA, Gloria GONZÁLEZ FUSTER, *et ál*. (2011: 87).

[1316] PROGRAMA DE ESTOCOLMO - UNA EUROPA ABIERTA Y SEGURA QUE SIRVA Y PROTEJA AL CIUDADANO (2010: 1). Así, en su resolución sobre el Programa de Estocolmo el Parlamento Europeo mantuvo una posición favorable a la elaboración de un régimen general de protección de datos en la UE. El Parlamento acogió con satisfacción un amplio sistema de protección de datos e invitó a la revisión de la Decisión marco 2008/977/JAI del Consejo. Pidió a la Comisión y a los Estados miembros que se asegurasen de que la futura acción de la UE respete los derechos fundamentales y «*procure un equilibrio adecuado entre la seguridad y la libertad, y que se supervise y racionalice adecuadamente este objetivo cree firmemente en la primacía del Estado de Derecho, el control jurisdiccional eficaz* (…)». En la RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2009, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada "Un espacio de libertad, seguridad y justicia al servicio de los

Específicamente en las observaciones formuladas por la Comisión Europea en su comunicación "Un enfoque global de la protección de los datos personales en la Unión Europea", de 4 de noviembre de 2010, de hecho, se pusieron de manifiesto los límites de la legislación y las políticas europeas, que se mostraban completamente insuficientes para asegurar una adecuada protección del derecho fundamental a la protección de los datos personales, sometida a un marco fragmentado en el que predomina la incertidumbre y el riesgo de violaciones y abusos que afectan a las decisiones de los consumidores y usuarios que, por el contrario, necesitan contar con reglas claras y controles adecuados[1317], y a lo que se suman los inadecuados regímenes para la transferencia de datos con terceros Estados. La Comunicación de la Comisión[1318] estimaba esencial que las normas que debían aplicar las autoridades nacionales, y que debían cumplir las empresas y los responsables del desarrollo de tecnologías, estuvieran claramente definidas de modo que permitiesen a los ciudadanos tener claros sus derechos.

6. Por eso, a fin de abordar los problemas y alcanzar los objetivos esenciales puestos de relieve por la Comisión Europea, se anunció que la misma presentaría propuestas legislativas destinadas a revisar el marco jurídico de la protección de datos, con el objetivo de reforzar

ciudadanos − Programa de Estocolmo", 25 de noviembre de 2009 – Estrasburgo, P7_TA(2009)0090. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009-0090+0+DOC+XML+V0//ES [consulta: 02 de febrero de 2017].

[1317] La Comunicación pone retos a continuación específicos, incluyendo la necesidad de: 1) abordar el impacto de las nuevas tecnologías (por ejemplo, la red social y la computación en nube); 2) reforzar la dimensión de mercado interior de la protección de datos; 3) hacer frente a la globalización y mejorar las transferencias internacionales de datos; 4) consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre protección de datos; 5) mejorar la coherencia del marco jurídico que regula la protección de datos. La comunicación concluía que, al igual que la tecnología, la forma en que los datos personales se utilizan y comparten en la sociedad está en evolución constante, se plantea a los legisladores el reto de establecer un marco legislativo que resista al tiempo y, en particular, que las normas europeas de protección de datos sigan asegurando un elevado nivel de protección y seguridad jurídica a las personas, a las Administraciones Públicas y a las empresas en el mercado interior, durante varias generaciones. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, (COM(2010) 609 final, págs. 3 y ss.

[1318] La Comunicación es el resultado de la auditoría realizada por la Comisión del marco jurídico actual, que comenzó con una Conferencia de Alto Nivel celebrada en Bruselas en mayo de 2009 y seguida por una consulta pública, consulta a los actores interesados, mediante conferencias, seminarios, grupos de trabajo que desembocan finalmente en la Resolución del Parlamento Europeo, de 6 de julio de 2011, que aprobó un informe favorable a reformar el marco de la protección de datos. *Vid*. RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)), 6 de julio de 2011 – Estrasburgo, P7_TA(2011)0323. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES [consulta: 03 de febrero de 2017]. Al mismo tiempo, se exploró la percepción pública a través de una encuesta Eurobarómetro realizada en 2010 y se encargaron una serie de estudios a grupos de expertos estudiosos de la materia. SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre, Brussels, June 2011, págs. 330. Los resultados de la encuesta evidenciaron que un alto porcentaje de ciudadanos europeos (70%) tenían una gran preocupación acerca de la posibilidad de que los datos personales que les conciernen, en poder de las empresas, sean utilizado para fines distintos de aquellos para los que fueron recogidos.

la situación de la UE en materia de protección de los datos personales en el contexto de todas las políticas de la UE[1319], incluso en los ámbitos de la prevención de la delincuencia y cumplimiento de la ley. Igualmente, la Comisión mencionó la necesidad de revisar las normas de protección de datos en el área de la cooperación policial y judicial en asuntos penales. Además, se anunció la adopción de «*medidas no legislativas, como la promoción de la autorregulación y el examen de la viabilidad de los distintivos europeos*» de protección de la privacidad.

7. Como se analizará por extenso, el "paquete de reformas" del marco general de la protección de datos personales en la Unión Europea presentado por la Comisión[1320], con el fin de establecer normas de protección de datos dentro del ELSJ, se articulaba en la adopción de dos actos legislativos diferentes: un Reglamento, diseñado para sustituir a la Directiva de 1995, que contiene los puntos de conexión que realizan la función de determinar la ley aplicable al tratamiento de los datos personales por parte de los Estados miembros de la Unión Europea y el Acuerdo sobre el Espacio Económico Europeo[1321]; y una Directiva dirigida a dictar normas sobre las cuestiones relativas a la seguridad interna e internacional de la Unión y Estados miembros. Las propuestas presentadas por la Comisión fueron el primer paso para crear un nuevo marco de protección de datos dentro de la UE.

8. Este "paquete" se presentó el 25 de enero de 2012 y consistía, tal y como se ha indicado, en una propuesta de Reglamento para sustituir a la Directiva 95/46/CE[1322], y de

[1319] La Comisión propuso una serie de compromisos clave como el incremento de la transparencia, más control de los individuos sobre sus datos personales, refuerzo de las normas de consentimiento, armonización de las condiciones de tratamiento de datos sensibles y establecimiento de sanciones y recursos eficaces.

[1320] Sobre las propuestas de reforma, *vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY - Working Party on Police and Justice (2009); EDPS (2011a), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011, págs. 36. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf [consulta: 04 de febrero de 2017]; EUROPEAN COMMISSION - Directorate-General Justice, Freedom and Security (2010), Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Final Report, 20 January 2010, págs. 57; COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, (COM(2010) 609 final.

[1321] En el escenario de la economía global resulta necesario definir paradigmas comunes, de la forma más amplia y coherente posible, de modo que conduzca al legislador europeo a implementar una política de regulación de los derechos de la persona cuya protección no se considere imputable únicamente a la capacidad de negociación de las partes, sobre todo con respecto a la protección de la privacidad del usuario. En este contexto, se revela cómo la posibilidad de trabajar en los mercados transnacionales exige la definición de reglas normativas comunes aplicables a todos los usuarios, independientemente de su nacionalidad.

[1322] PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación

una propuesta de Directiva que regula el tratamiento de datos personales en los sectores justicia y la policía[1323] (sectores excluidos del ámbito de aplicación de la Directiva 95/46/CE). La iniciativa de revisión, que forma parte del programa denominado "Agenda Digital para Europa"[1324] y, en general, como parte de la "Estrategia Europa 2020"[1325], está orientada a la consecución de dos objetivos principales: por un lado, fortalecer el derecho a la protección de datos personales como un derecho fundamental, como se establece en la CDFUE (artículo 8) y el Tratado de Lisboa (artículo 16 del TFUE) que requiere que sea garantizada un eficaz y uniforme protección de los ciudadanos europeos sobre todo el territorio europeo, proporcionando a los ciudadanos un control efectivo sobre sus datos personales[1326]; por el otro, promover la consolidación del mercado único digital europeo[1327], fomentando la creación de nuevas oportunidades de negocio y trabajo en el campo de la economía digital, y el aumento de la confianza de los ciudadanos en los servicios en línea[1328].

---

de estos datos (Reglamento general de protección de datos), Bruselas, 25.1.2012, COM/2012/011 final, 2012/0011 (COD). Disponible en Internet: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf [consulta: 04 de febrero de 2017].

[1323] PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, Bruselas, 25.1.2012, COM/2012/010 final, 2012/0010 (COD). Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0010 [consulta: 05 de febrero de 2017].

[1324] COMUNICACIÓN, DE 19 DE MAYO DE 2010, DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, titulada «Agenda digital para Europa» [COM(2010) 245 final - no publicada en el Diario Oficial]. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:si0016 [consulta: 05 de febrero de 2017].

[1325] COMUNICACIÓN DE LA COMISIÓN, de 3 de marzo de 2010, denominada Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador [COM(2010) 2020 final – no publicada en el Diario Oficial]. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:em0028 [consulta: 05 de febrero de 2017].

[1326] *Cfr*. sobre el tema Hielke HIJMANS (2016), *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer International Publishing, págs. 604. El primer motivo que condujo a la Comisión Europea a tomar medidas en este asunto con un paquete tan ambicioso, ya ampliamente debatido, se encuentra en una necesidad apremiante y fuerte de armonización de las decisiones tomadas con la Directiva de 1995 sobre el tratamiento de datos personales, que, sin duda, había logrado el objetivo de una primera armonización. Sin embargo, en el momento de su puesta en práctica y desarrollo por los Estados miembros fueron en direcciones diferentes, interpretando y desarrollando los parámetros europeos en términos bastante distintos. El resultado ha sido una sorprendente diversidad de normas y niveles de protección para las personas, así como inconsistencias y dificultades para las empresas que operan.

[1327] El mercado único digital es uno de los objetivos que la Unión Europea se ha fijado y en su puesta en práctica las instituciones europeas están introduciendo importantes intervenciones reguladoras. Se trata de crear un mercado único en todo el territorio de la Unión, a saber, la eliminación de las barreras y obstáculos que impiden o reducen las transacciones económicas, principalmente el intercambio de servicios entre empresas de Estados miembros diferentes. Sintéticamente se puede definir como la eliminación de las barreras nacionales a las transacciones que se desarrollan *on line* dentro de la Unión, con el fin último de incrementar la prosperidad económica y contribuir cada vez más a una estrecha y eficaz unión entre los Estados miembros. «Mercado único digital. Derribar barreras para aprovechar las posibilidades que ofrece internet», en *Comisión Europea*. Disponible en Internet: https://ec.europa.eu/commission/priorities/digital-single-market_es [consulta: 05 de febrero de 2017].

[1328] El segundo aspecto, proviene del incesante y frenético desarrollo de nuevas tecnologías que cambian la raíz de nuestra sociedad. Esta situación se encuentra en general en relación con todo tipo de actividades en el ámbito de las TIC, la evolución de las redes de Internet, los enormes flujos cada vez más intensos de

9. Por ello, el fortalecimiento del derecho a la protección de datos personales se ha convertido en un objetivo principal, dotado de valor intrínseco, de las propuestas formuladas por la Comisión Europea en 2012 relativas a la consecución de un marco legal europeo renovado de la protección de datos. Se trata, sin duda, de la búsqueda de una adecuada protección de los datos personales, lo que requiere una prueba de proporcionalidad entre los medios de seguridad pública y de la privacidad, reafirmando el valor central de esta última como de un área prioritaria para la verificación de los principios del Estado de Derecho en la Unión Europea. Por eso, la falta de armonización legislativa sistémica ha llevado a la presencia, en cada Estado miembro, de diferentes líneas de interpretación y diferentes orientaciones de la aplicación que, si bien se refieren a los aspectos individuales y limitados de protección de datos, han conducido a una aplicación desigual y la coexistencia de diferentes niveles de seguridad. Estos márgenes de discrecionalidad ejercida por los Estados miembros, a la que se suman los ámbitos en las que la Directiva de 1995 no interviene, han actuado de forma que los Estados han legislado en este ámbito según su propia conveniencia.

10. Sobre la propuesta de Directiva, la Comisión Europea comentó en su Comunicación de 2012 que la cooperación transfronteriza en asuntos policiales exigía ciertas mejoras[1329]. En el pasado, la Comisión, que no tenía poderes ejecutivos sobre la Decisión Marco del Consejo de 2008, no consiguió evitar la aparición de un mosaico de reglamentaciones muy variadas en los distintos Estados miembros. En el proceso de reforma, se consideró que una directiva constituía el instrumento ideal para garantizar cierta armonización en el campo de la cooperación policial y judicial en materia penal y, al mismo tiempo, dejar un nivel de flexibilidad necesaria a los Estados miembros[1330]. La propuesta de Directiva tenía por objeto

información personal, los *outsourcing* ubicados en cualquier parte del mundo, la nube, redes sociales, motores de búsqueda y por últimos, pero no menos importantes, los "*Big Data*" y las nuevas técnicas de vigilancia masiva. Todos han puesto de manifiesto las limitaciones de la disciplina europea que no ayuda a identificar plenamente la legislación aplicable (legislación nacional o de terceros países) a una determinada actividad, la distribución de las responsabilidades contractuales y no contractual, y a hacer efectivo el ejercicio de los derechos por parte de los interesados. Como señaló la entonces Comisaria de Justicia y vicepresidenta de la Comisión Europea, Viviane Reding, con ocasión de la presentación del proyecto de reforma, de hecho, en el momento de la entrada en vigor de la Directiva 95/46/CE relativa a la protección de datos personales, menos del uno por ciento de los europeos hizo uso de Internet. En cambio, hoy en día, en contraste, casi el total de los ciudadanos europeos tiene un acceso a la red, donde se pueden intercambiar y se transfieren grandes cantidades de datos en fracciones simples de un segundo. También la llegada de las redes sociales expone la privacidad de los usuarios a nuevas y formas peligrosas de control y la interferencia, que pueden tener repercusiones potencialmente negativas sobre el funcionamiento social, familiar y del trabajo. COMISIÓN EUROPEA - Comunicado de Prensa (2012), La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas, Bruselas, 25 de enero de 2012. Disponible en Internet: http://europa.eu/rapid/press-release_IP-12-46_es.htm [consulta: 06 de febrero de 2017].

[1329] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO (2012).

[1330] Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016), «The New Police and Criminal Justice Data Protection Directive: A First Analysis», en *New Journal of European Criminal Law*, vol. 7, issue 1, pág. 9.

garantizar un alto nivel de protección de datos en el ámbito cooperación policial y judicial en materia penal, a fin de aumentar la confianza mutua entre los órganos judiciales y policiales de los distintos Estados miembros y facilitar la cooperación entre las autoridades nacionales que intercambian datos en toda la UE, lo que resulta muy oportuno a la luz de los recientes ataques terroristas de los últimos años[1331].

11. El ambicioso plan de reforma de la Comisión, que pretende asegurar normas comunes ("*jus commune*") y un nivel uniforme de protección de datos personales en la Unión, parece estar lejos de ser exhaustivo. Aunque el proyecto trata de ser un instrumento de respuesta válido normalizando el uso de los datos personales de forma más precisa quee la normativa anterior, no proporciona una solución a muchos de los problemas relacionados con esta materia. Los textos son el pacto final resultante de la convergencia de múltiples tensiones políticas entre ideologías e intereses en el que han confluido grupos de presión de manera incesante y feroz. Es difícil encontrar normas de la Unión Europea que hayan recibido tanta presión de los lobbies y tantas enmiendas, de lo que se deduce el largo proceso de gestación que precedió su aprobación, lo cual vamos a examinar. De hecho, aunque lo que busca la reforma es precisamente la armonización y modernización de la legislación europea existente sin dejar, por un lado, el fortalecimiento de los derechos de las personas y, en segundo lugar, la garantía de un alto grado de protección en el ámbito de la cooperación judicial y policía, en algunas de las disposiciones en que se concreta esta reforma, las

Disponible en Internet: http://journals.sagepub.com/doi/abs/10.1177/203228441600700102 [consulta: 06 de febrero de 2017]. A diferencia del tratamiento de datos personales generales, el tratamiento relacionado con la seguridad requiere un cierto nivel de flexibilidad. Por ejemplo, es posible que no se observen estrictos requisitos de calidad de los datos cuando los datos de seguridad a menudo se basan en rumores, información de fuentes encubiertas y rumores. O bien, el principio de la limitación de fines puede no aplicarse estrictamente, porque la información recopilada en un caso particular puede encontrar usos inesperados para resolver otros casos en el futuro cercano o no tan próximo. O bien, el derecho a la información y el acceso, si se ejerce en la medida de lo posible, prácticamente haría que cualquier operación policial quedase desactivada. Esta es la razón por la cual las necesidades especiales relacionadas con la seguridad deben ser acomodadas en un texto relevante de protección de datos; la tarea de encontrar un equilibrio entre los objetivos de protección de datos y los objetivos de la política de seguridad es delicada y ciertamente difícil.

[1331] John BOWMAN (2015), «Paris Attacks Bring "Police" Directive Negotiations Back Into Spotlight», en *International Association of Privacy Professionals*, Feb 6. Disponible en Internet: https://iapp.org/news/a/paris-attacks-bring-police-directive-negotiations-back-into-spotlight/ [consulta: 07 de febrero de 2017]. En la Unión Europea, la actualidad del tema de una reconciliación entre la protección a la vida privada y la necesidad de seguridad y prevención de los fenómenos terroristas se añadió al debate, como sabemos, después del 11 de septiembre de 2001, cuando se generalizó la consideración de que la privacidad y protección de datos pueden ser limitados en la lucha contra el terrorismo y el crimen, ganando el apoyo de muchos gobiernos. Después de los ataques terroristas de Madrid y Londres, y en los últimos tiempos con los atentados de París, Bruselas, Berlín, Londres y Barcelona, el intercambio de datos personales entre las autoridades policiales en varios Estados miembros de la UE se ha convertido en un elemento esencial de la cooperación internacional contra el terrorismo y el crimen organizado. Estos dramáticos acontecimientos, hacen que sea una vez más extraordinariamente actual el tema de la recopilación de la información y de grandes bases de datos gestionadas por operadores públicos (y privados) a menudo utilizadas, como en el caso de los sistemas de reservas aéreas, para el propósito de seguridad y prevención del delito.

posiciones son divergentes. Como consecuencia, nos encontramos con normas que encapsulan difíciles consensos en múltiples aspectos, paradójicas, incompletas e imprecisas en ocasiones.

12. La reforma se basa en dos instrumentos legislativos diferentes (reglamento y directiva), que contienen dos niveles de protección diferentes[1332], con claras discrepancias en términos de garantías para los ciudadanos. De este modo desaparece la posibilidad de construir un marco único y coherente que garantice un alto nivel de seguridad en los Estados miembros. A esto se suma la existencia de una geometría variable en las acciones de cooperación policial, en virtud de las disposiciones especiales que goza el Reino Unido, Irlanda y Dinamarca, un factor que complica aún más la situación.

13. De todas formas, la reforma tiene un impacto considerable y deliberado en la regulación práctica del tratamiento de datos personales, y no proviene de un interés contingente y ocasional, sino que forma parte de un camino lento y complicado para repensar el "*status quo ante*"[1333]. Sería difícil, por otra parte, no reconocer el alcance de las innovaciones introducidas. Por esta razón, a la vista del proceso regulatorio europeo e internacional y de la jurisprudencia de los tribunales, el surgimiento del "nuevo" derecho a la protección de datos personales como un caso complejo, hace falta aquí examinar sus perspectivas de desarrollo futuro, del marco general tan delineado gracias cual la Unión Europea ve tener la oportunidad de responder a las diversas cuestiones relacionadas con el equilibrio del derecho a la protección de datos personales con las necesidades de seguridad colectivas obligatorias y la prevención del delito.

[1332] Asimismo, el hecho de que la propuesta de Directiva no haya sido adoptada en forma de reglamento ha comportado críticas también por parte del Parlamento Europeo, que «(…) *considera que la propuesta de directiva en el ámbito de la cooperación judicial en materia penal y la cooperación policial debe ser más ambiciosa y contemplar salvaguardas más contundentes* (…)». RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 22 de mayo de 2012, sobre la Estrategia de Seguridad Interior de la Unión Europea (2010/2308(INI)), Martes 22 de mayo de 2012 - Estrasburgo, P7_TA(2012)0207, apartado 26. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0207+0+DOC+XML+V0//ES [consulta: 07 de febrero de 2017].

[1333] Dicho esto, aunque con dificultad y con una gran cantidad de egoísmo por parte de los Estados miembros (siempre más "Estados" y cada vez menos europeos), el uso de reglamento siempre ha sido bastante polémico y debatido en las instituciones europeas, y en el caso de la reforma de la Directiva 95/46/CE sobre la privacidad, incluso más. Para los partidarios, de la Unión Europea, la "herramienta" del reglamento debe ser cada vez más utilizada, llegando a la cesión de los parlamentos nacionales hacia las instituciones europeas; en cambio, para aquellos que abogaban el mantenimiento o incluso el fortalecimiento de los Estados nacionales y su plena soberanía, la directiva sigue siendo la mejor manera de legislar sobre principios comunes, dejando la libertad de maniobra de los Estados-nación que necesitan de la transposición de las directivas. No es casualidad que, durante el largo debate que precedió la adopción del RGPD, el Reino Unido fue el oponente más acérrimo de la utilización del RGPD y, unos meses más tarde, surgió el *Brexit*.

14. Por lo tanto, antes de analizar los nuevos aspectos clave que más interesan a la presente investigación y del por qué del "paquete de reformas" (Reglamento (UE) 2016/679 y Directiva (UE) 2016/680) es necesario prestar atención, en primer lugar, al largo y tortuoso *iter* legislativo[1334] –dada la dificultad de conciliar las diferentes necesidades que inspiraron las distintas legislaciones nacionales[1335]– que concluyó con la aprobación final por el Parlamento Europeo, en sesión plenaria, el 14 de abril de 2016[1336], del texto de la posición adoptada en primera lectura por el Consejo de la UE sobre la propuesta de Reglamento relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[1337], así como del texto de la posición adoptada en primera lectura por el Consejo sobre la propuesta de Directiva sobre transmisión de datos para cuestiones judiciales y policiales[1338], y su siguiente publicación en el Diario Oficial de la Unión Europea del 4 de mayo de 2016.

[1334] El proceso legislativo ha padecido un estancamiento momentáneo junto con el final de la legislatura y las nuevas elecciones para el Parlamento Europeo celebradas en mayo de 2014 y la consiguiente renovación de la composición de la Comisión.

[1335] El progreso de la reforma se ha visto frenado por el Reino Unido y, lo que es más sorprendente, por los intentos obstruccionistas de Alemania y Suecia, por temor a que las nuevas normas impongan cargas excesivas a las empresas. *Amplius*, Raegan MACDONALD (2013), «Human Rights Day: EU's Data Protection Reform: restoring trust by reinforcing user rights», en *accessnow.org*, 10 December. Disponible en Internet: https://www.accessnow.org/human-rights-day-eus-data-protection-reform-restoring-trust-by-reinforcing/ [consulta: 08 de febrero de 2017].

[1336] PARLAMENTO EUROPEO - Notas de prensa (2016b), Reforma de la protección de datos - Nuevas reglas adaptadas a la era digital, 14-04-2016, http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/Reforma-de-la-protecci%C3%B3n-de-datos-%E2%80%93-Nuevas-reglas-adaptadas-a-la-era-digital; EUROPEAN COMMISSION - Statement (2016b), Joint Statement on the final adoption of the new EU rules for personal data protection, Brussels, 14 April 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm [consulta: 08 de febrero de 2017].

[1337] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), *Diario Oficial de la Unión Europea*, L 119, 4.5.2016, págs. 1–88. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679 [consulta: 08 de febrero de 2017].

[1338] DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, *Diario Oficial de la Unión Europea*, L 119, 4.5.2016, págs. 89–131. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.SPA&toc=OJ:L:2016:119:TOC [consulta: 08 de febrero de 2017]. El ámbito territorial de la Directiva se extiende más allá de los 28 Estados miembros de la UE, incluyendo también a los países del Espacio Económico Europeo (EEE) como Islandia, Liechtenstein y Noruega. *Vid*. «Acuerdo sobre el Espacio Económico Europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:em0024 [consulta: 08 de febrero de 2017]. El Acuerdo entró en vigor el 1 de enero de 1994. Debe recordarse que el 27 de abril de 2016 se aprobó la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de relativa a la utilización de datos del registro de nombres de los pasajeros (*PNR*) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (vid. *supra*), con transposición a más tardar el 25 de mayo de 2018.

15. En segundo lugar, debido al enorme alcance de estos instrumentos normativos que conforman el nuevo marco de la protección de datos en la UE, se hace necesario centrar el análisis en las principales características innovadoras y los temas más controvertidos de cada uno de los dos actos legislativos de forma individual, atendiendo al objeto de la presente investigación, que son la relación de la protección de datos con las medidas de seguridad y orden público, en particular aquellas adoptadas en la lucha contra el terrorismo, que, en ningún caso, pueden justificar una medida de retención de datos generalizada[1339]. En efecto, los Estados no pueden adoptar las medidas que consideren apropiadas, aunque estén justificadas para luchar contra el terrorismo, sin tener garantías adecuadas y efectivas contra los abusos[1340] y el mantenimiento o el refuerzo de esas medidas debe explicarse y justificarse convincentemente[1341]. A la luz de lo anterior, por lo tanto, intentaremos contestar a la siguiente pregunta: ¿Cómo consigue la nueva reforma de protección de datos garantizar los derechos de privacidad frente a las necesidades que se derivan de la seguridad pública en la lucha contra el terrorismo y otros delitos graves?

2. La complicada armonización de la nueva legislación europea de protección de datos

16. La estructura básica de la nueva normativa en materia de protección de datos, es el fruto de la negociación desarrollada a partir de la propuesta de la Comisión Europea que se llevó a cabo dentro de los diálogos tripartitos[1342] que modificaron en profundidad la propuesta original de la Comisión. En efecto, a lo largo de los años, la propuesta de Reglamento ha sido objeto de continuas intervenciones y modificaciones que han erosionado y alterado el contenido de la propuesta original y las intenciones de los primeros redactores. De hecho, de acuerdo con algunos críticos, se trata de uno de los actos legislativos con mayores presiones en la historia del Parlamento Europeo[1343]: los eurodiputados han votado más de cuatro mil enmiendas –muchas de las cuales acogen plenamente las sugerencias de

[1339] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartados 42 y 51.
[1340] TEDH, *Klass y otros contra Alemania*, apartado 42.
[1341] TEDH, *Nada contra Suiza*, apartado 186.
[1342] Parlamento Europeo y del Consejo de la UE, que participan sobre un plan paritario al procedimiento de legislación, han introducido en los últimos años una serie de enmiendas a los textos presentados por la Comisión Europea. Como veremos, varios han sido también las contribuciones del Grupo de Trabajo y del SEPD, que han emitidos dictámenes y documentos sobre la reforma.
[1343] Nikolaj NIELSEN (2016), «EU parliament passes grand data protection law», en *EUobserver*, Brussels, 14 Apr. Disponible en Internet: https://euobserver.com/justice/133060 [consulta: 09 de febrero de 2017].

los gigantes de la tecnología con sede en los EE.UU. – y se desarrolló una campaña de presión que acabó con la mayor parte de las ambiciones que contenía el texto original[1344].

17. El intento del legislador europeo era establecer una base común, dinámica y flexible, capaz de adaptarse a los cambios tecnológicos sin perder su eficacia. Con esta premisa del carácter dinámico y adaptativo de la normativa a elaborar, los organismos de la UE, los Estados miembros y las autoridades nacionales de control desarrollaron un esfuerzo coordinado para proceder a la definición de estas normas en todos sus detalles. Por lo tanto, el mecanismo diseñado por la nueva normativa europea pretende garantizar el mantenimiento constante en el tiempo de "adecuación" de la protección de datos personales, es decir, una perspectiva de eficacia duradera, garantizando a las personas físicas el control de sus datos personales y fortalecer la certeza jurídica y operativa de las autoridades públicas y los agentes económicos. Por otro lado, debe tenerse en cuenta que cuando las propuestas fueron presentadas, entre el 2012 y 2014, la Unión Europea había dejado de lado el miedo al terrorismo y la urgencia de tener un alto nivel de seguridad interior. Posteriormente, sin embargo, debido a los graves casos terroristas ocurridos después, el miedo y el retorno a las medidas de seguridad invasivas en la esfera de las libertades del individuo dictan la agenda política y no ha sorprendido que algunos Estados se hayan situado en un orden jurídico de excepción con fuertes restricciones en el ámbito de las libertades y derechos fundamentales.

18. La reforma trata de abordar la necesidad de fortalecer el sistema de protección de la privacidad de los ciudadanos y la necesidad de apoyar y facilitar las actividades de las fuerzas de seguridad, a través de un flujo más fácil de datos personales entre las autoridades competentes, también para combatir y prevenir incidentes terroristas. Esto, si bien puede facilitar la prevención del delito y garantizar la seguridad pública, por el contrario, también puede derivar en una degeneración del control (aunque fuese originalmente legítima, oportuna y fundada) con una vigilancia de carácter masivo[1345]. Especialmente en un

[1344] Así ha afirmado la asociación *European Digital Rights (EDRi)*, que defiende los derechos de los consumidores digitales. En particular, véanse Joe MCNAMEE (2016), «Press Release: Vote on Data Protection and Passenger Name Record package», en *European Digital Rights (EDRi)*, 13 Apr 2016. Disponible en Internet: https://edri.org/press-release-data-protection-and-passenger-name-record-package-to-be-voted-on-tomorrow/ [consulta: 09 de febrero de 2017].

[1345] En esta línea, el Parlamento Europeo en sus recientes resoluciones, lanza la alarma sobre la vigilancia electrónica masiva a la que están sometidos los ciudadanos de la UE, obviamente, no destinados a disminuir a pesar de las sentencias del TJUE. Se remarca que la respuesta hasta ahora ha sido muy insuficiente y los derechos fundamentales de los ciudadanos de la UE todavía están en peligro debido a que se ha hecho muy poco para asegurar su plena protección. Por otra parte, el Parlamento precisa que algunos Estados, como Francia, el Reino Unido y los Países Bajos, han adoptado nuevas leyes sobre la inteligencia que generan preocupación. Las resoluciones invitan a formular una estrategia de la UE para una mayor independencia informática y mayor privacidad en la web y ponen de relieve la necesidad de garantizar un control democrático

momento como el presente, en el que el binomio libertad-seguridad se está redefiniendo con dificultad, surge la conciencia de que los riesgos exponen a una idea de seguridad arbitraria frente a la que deben protegerse las democracias.

2.1. La falta de armonización de las propuestas presentadas por la Comisión Europea

19. La aprobación de los dos textos legislativos –precedido por un primer consentimiento favorable del Parlamento Europeo y del Consejo de la UE en 2011, que participan sobre un plan paritario al procedimiento legislativo (definido "ordinario", según el TFUE)[1346]–, es el último acto de un proceso iniciado el 25 de enero de 2012, cuando la Comisión adoptó un "paquete" de medidas para la reforma de las normas de la UE sobre protección de datos[1347],

y eficaz de las actividades de inteligencia, así como la necesidad de reconstruir la confianza con los EE.UU. La vigilancia electrónica masiva pone en peligro los derechos individuales y debe ser limitada. Por esto se debe prestar gran atención al tratamiento de datos personales, derecho que supervisa el TJUE que, –como hemos visto, tanto con la sentencia *Digital Rights Ireland* de 8 de abril 2014, que declaró inválida la Directiva 2006/24/CE, como con la sentencia *Schrems* de 6 de octubre de 2015, con el que ha rechazado la Decisión 2000/520/CE– hace todos los esfuerzos posibles para salvaguardar los derechos fundamentales de los ciudadanos. El Parlamento Europeo también ha pedido a los Estados adoptar una definición común de la seguridad nacional, invocando una estrategia de lucha contra el terrorismo tan rigurosa como tan capaz de poner al centro derechos y libertades. Sobre todo, porque no todas las limitaciones de la libertad son realmente eficaces para hacernos más seguros. *Vid*. RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 29 de octubre de 2015, sobre el seguimiento de la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la vigilancia electrónica masiva de los ciudadanos de la UE (2015/2635(RSP)), Jueves 29 de octubre de 2015 - Estrasburgo, P8_TA(2015)0388. La Resolución ha sido adoptada con 342 sí, 274 no, y 29 abstenciones. También Resolución del Parlamento Europeo, de 25 de noviembre de 2015, sobre la prevención de la radicalización y el reclutamiento de ciudadanos europeos por organizaciones terroristas (2015/2063(INI)), Miércoles 25 de noviembre de 2015 - Estrasburgo, P8_TA(2015)0410. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0410+0+DOC+XML+V0//ES [documentos consultados: 10 de febrero de 2017].

[1346] El "paquete de reformas" sobre la protección de los datos, gracias a las innovaciones introducidas por el Tratado de Lisboa, ha sido adoptado por el procedimiento de colegislación que prevé una participación paritaria del Parlamento Europeo y del Consejo, la Unión Europea (trílogos). Así pues, la Comisión antes y el Parlamento Europeo luego, de conformidad con los principios de subsidiariedad y proporcionalidad, decidieron articular la reforma a través de un reglamento, elección que fue considerada como la más efectiva y apropiada para redefinir el marco jurídico de la protección de los datos personales en la UE vista de la reducción de la fragmentación jurídica. Sin embargo, por las mismas razones relacionadas con las dificultades de conciliación de las diferentes necesidades que inspiraron las distintas leyes nacionales, incluso el proceso de aprobación de esta propuesta ha tenido largos retrasos significativos (2012-2016). También en esta ocasión el planteamiento europeo no encuentra fácil armonización con las diferentes experiencias que surge en el marco jurídico global. Sobre los principios de subsidiariedad y proporcionalidad, artículo 5 del TUE (antiguo artículo 5 TCE), apartado 3: «*En virtud del principio de subsidiariedad, en los ámbitos que no sean de su competencia exclusiva, la Unión intervendrá sólo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional y local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión. Las instituciones de la Unión aplicarán el principio de subsidiariedad de conformidad con el Protocolo sobre la aplicación de los principios de subsidiariedad y proporcionalidad. Los Parlamentos nacionales velarán por el respeto del principio de subsidiariedad con arreglo al procedimiento establecido en el mencionado Protocolo*»; y apartado 4: «*En virtud del principio de proporcionalidad, el contenido y la forma de la acción de la Unión no excederán de lo necesario para alcanzar los objetivos de los Tratados. Las instituciones de la Unión aplicarán el principio de proporcionalidad de conformidad con el Protocolo sobre la aplicación de los principios de subsidiariedad y proporcionalidad*».

[1347] Así escribió la Comisión en la Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: «*En este nuevo entorno digital, los ciudadanos tienen derecho a ejercer un control efectivo sobre su información personal. La protección de datos es en Europa un derecho*

que incluye, como se ha indicado, una propuesta de Reglamento COM (2012)11 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), para sustituir a la Directiva 95/46/CE, y una propuesta de Directiva COM (2012)10 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, para reemplazar a la Decisión Marco 2008/977/JAI del Consejo.

20. La propuesta de reforma[1348] no cubría los temas relacionados con el contexto específico de las comunicaciones electrónicas relacionadas con el uso del *PNR* (*vid. supra* Directiva *PNR*). También se quedaba fuera del ámbito la política exterior y de seguridad común que tiene una base jurídica diferente en el artículo 39 del TUE[1349]. La propuesta de la Comisión incluía también al sector público debido al creciente intercambio transfronterizo en áreas tales como fiscalidad, seguridad social, salud, bancos y supervisión del mercado financiero.

21. Como es bien sabido, el reglamento de la Unión es directamente aplicable de manera uniforme en todo el territorio europeo y, como acto de "*self-executing*" (según el artículo

fundamental consagrado tanto en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea, por lo que debe salvaguardarse adecuadamente (…)*. Es preciso disponer en toda la UE de normas modernas y coherentes que permitan la libre circulación de datos entre los Estados miembros. Las empresas necesitan reglas claras y uniformes que aporten seguridad jurídica y reduzcan las cargas administrativas. Así lo exigen el funcionamiento del mercado único y la necesidad de estimular el crecimiento económico, crear puestos de trabajo y fomentar la innovación. Una modernización de la normativa de la UE en materia de protección de datos que potencie la dimensión de mercado interior garantizará a los ciudadanos un alto nivel de protección de datos y fomentará la seguridad, la claridad y la coherencia jurídicas. Por lo tanto, ocupa un lugar destacado en el Plan de Acción de Estocolmo de la Comisión Europea, en la Agenda Digital para Europa y, de forma más general, en la estrategia de crecimiento de la UE Europa 2020*». *Cfr*. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI, Bruselas, 25 de enero de 2012, COM/2012/09 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0009 [consulta: 11 de febrero de 2017].

[1348] El ponente de la propuesta de Reglamento fue el Eurodiputado Jan-Philipp Albrecht (Verdes, Alemania), en cambio con respecto a la propuesta de Directiva el ponente fue el Eurodiputado Dimitrios Droutsas (S&D, Grecia).

[1349] Artículo 39 del TUE: «*De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes*».

288 del TFUE)[1350], es directo e inmediatamente ejecutivo y no necesita el recibimiento de parte de los Estados miembros, resultando aplicable desde el momento en que es aprobado. Formalmente se sitúa por encima de todas las otras fuentes de derecho interno, con exclusión de la Constitución, sobre la base de un principio bien consolidado de la primacía de la legislación de la UE sobre las leyes nacionales. Por lo tanto, en caso de conflicto, contradicción o incompatibilidad entre las normas del Reglamento y las nacionales, las primeras prevalecerán sobre las segundas[1351]. En línea con el enfoque pragmático elegido por la Comisión Europea, se ha reconocido a los Estados miembros y a las autoridades competentes en la materia un cierto margen de maniobra para mantener o adoptar, de conformidad con el RGPD, las normas específicas en este ámbito[1352]. Debe tenerse en cuenta que el RGPD se diseñó para que entrase en vigor dos años después de su publicación en el Diario Oficial de la UE, con el fin de dar tiempo suficiente a los Estados miembros y a los ciudadanos a que se adaptasen a las nuevas reglas.

[1350] Artículo 288 (antiguo artículo 249 TCE) del TFUE: «*Para ejercer las competencias de la Unión, las instituciones adoptarán reglamentos, directivas, decisiones, recomendaciones y dictámenes. El reglamento tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro. La directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios. La decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos. Las recomendaciones y los dictámenes no serán vinculantes*». Los reglamentos siempre tienen un efecto directo. El artículo 288 del TFUE efectivamente señala que los reglamentos son directamente aplicables en los países de la UE. El efecto directo del Derecho europeo fue consagrado por el TJUE en la sentencia *Van Gend en Loos* del 5 de febrero de 1963. El mismo Tribunal indica en la sentencia *Politi* del 14 de diciembre de 1971 que se trata de un efecto directo completo de los reglamentos. *Vid*. «El efecto directo del Derecho europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14547 [consulta: 11 de febrero de 2017].

[1351] «*El principio de primacía es válido para todos los actos europeos de aplicación obligatoria*» y, en consecuencia, «*los Estados miembros no pueden aplicar una norma nacional contraria al Derecho europeo*». Ese principio de primacía, al igual que el principio de efecto directo, no está inscrito en los tratados, pero ha sido consagrado por el TJUE en la sentencia *Costa contra Enel* del 15 de julio de 1964. *Vid*. «Primacía del Derecho europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14548 [consulta: 11 de febrero de 2017].

[1352] El Consejo de Ministros Español aprobó un Proyecto de Ley Orgánica de Protección de Datos, que adaptará la legislación española a las disposiciones del Reglamento General de Protección de Datos de las personas físicas UE 2016/679. En el caso de España, donde la protección de datos es un derecho fundamental protegido por el artículo 18, apartado 4, de la Constitución, la adaptación de nuestra legislación al RGPD hace necesaria la elaboración de una nueva Ley Orgánica en sustitución de la actual, cuyas normas y desarrollo deberán ser revisadas y adaptadas para evitar contradicciones. Igualmente, la AEPD ha desarrollado cuestiones concretas que el Reglamento comunitario remite a las autoridades nacionales de control y ha revisado sus tratamientos de datos personales para adaptarlos a esas exigencias. *Vid*. «El Gobierno aprueba el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal», en *Diario la Ley*, 10-11-2017. La AEPD publicó una serie de documentos con el fin de ayudar a los responsables de datos a cumplir con los requisitos del nuevo RGPD. Los documentos mencionados proporcionan pautas a las entidades que procesan datos personales para que puedan comenzar a adaptar sus procesos a fin de cumplir con los nuevos requisitos establecidos por el RGPD durante este período de transición. *Vid*. «Reglamento General de Protección de Datos», en *AEPD*. Disponible en Internet: https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php.

22. Las propuestas de la Comisión de 2012 tenían una base jurídica tripartita [1353]. En primer lugar, se refiere a la técnica mencionada por el artículo 16, apartado 2, del TFUE que, como se ha comentado, atribuye una competencia legislativa específica al Parlamento Europeo y al Consejo[1354], retomando los términos utilizados por el artículo 8 de la Carta de Niza. Debe recordarse que la Decisión Marco 2008/977/JAI no cumple con los criterios del artículo 16 del TFUE, ya que no es de aplicación en las actividades de tratamiento de datos personales puramente internas y, además, excluye la participación del Parlamento Europeo. Por eso, cuando el Tratado de Lisboa entró en vigor, surgió la necesidad de modificar o reemplazar la Decisión Marco 2008/977/JAI[1355]. Retomando el artículo 8 de la Carta, este último, elevando el derecho a la protección de datos personales como derecho fundamental de la Unión Europea, constituye la segunda parte de la base jurídica de la reforma propuesta[1356]. Por último, en la redacción de ambas propuestas hay referencias al artículo 8 del CEDH, que, como hemos visto, forma parte integrante de la legislación de la UE, y afecta a las diversas cuestiones jurídicas planteadas en este asunto.

23. Si bien el SEPD había emitido, en un primer momento, una opinión positiva sobre la propuesta de Reglamento[1357], la opinión sobre la propuesta de Directiva fue de carácter

[1353] La Comisión Europea es la institución encargada del inicio de los actos legislativos: prepara la propuesta legislativa y la somete al Parlamento Europeo y al Consejo de la Unión Europea. El Parlamento y el Consejo son las instituciones que tienen a sus cargos la responsabilidad de aprobar (aportando eventuales enmiendas) las propuestas recibidas por la Comisión. En cambio, el procedimiento legislativo ordinario es el principal procedimiento de aprobación de leyes en la Unión Europea. Asigna el mismo poder al Parlamento y al Consejo sobre la aprobación (o rechazo) de las propuestas de la Comisión. En fin, de acuerdo con el procedimiento legislativo ordinario, la Comisión Europea ha presentado contextualmente su propuesta legislativa al Parlamento Europeo y al Consejo de la UE para la primera lectura. *Vid*. «Ordinary legislative procedure», en *European Parliament*. Disponible en Internet: http://www.europarl.europa.eu/external/html/legislativeprocedure/default_en.htm [consulta: 12 de febrero de 2017].

[1354] Artículo 16, apartado 2, del TFUE: «*El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes*».

[1355] *Amplius*, Hielke HIJMANS and Alfonso SCIROCCO (2009), «Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?», en *Common Market Law Review*, vol. 46, issue 5, págs. 1515 y ss. Disponible en Internet: http://www.ivir.nl/publicaties/download/1711.pdf [consulta: 13 de febrero de 2017]. *Cfr*. en este sentido, también el apartado de esta investigación sobre la Decisión Marco 2008/977/JAI.

[1356] Gloria GONZÁLEZ FUSTER (2014b).

[1357] Así comentaba el anterior SEPD Peter Hustinx: «*The proposal for the general rules on data protection is ambitious and constitutes a huge step forward for data protection in Europe. Although there is certainly room for further improvement, we generally support the solutions proposed by the Commission. This proposal is an excellent starting point for the adoption of European rules on data protection robust enough to face the information technology-driven challenges before us*». En EDPS - Press Release (2012), EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice área, EDPS/02/12, Brussels, Wednesday 25 January 2012.

crítico[1358]. También crítica fue la siguiente y más precisa opinión del SEPD, sobre todo por la elección hecha por la Comisión que de ninguna manera podía interpretarse como un paso hacia un sistema uniforme de protección de datos. En otras palabras, según la opinion del SEPD se señala el riesgo de que los dos instrumentos normativos padeciesen una evolución disconforme o que pudieran distanciarse considerablemente en el nivel adecuado de protección, creando discrepancias y problemas de coordinación[1359]. Asimismo, el SEPD, es decididamente crítico respecto a la propuesta de Directiva, con respecto a la que afirma que, en muchos casos, se distancia de las disposiciones del Reglamento sin una motivación real, introduciendo elementos contrarios a la salvaguardia de los datos personales. En particular, el Supervisor lamenta la falta de claridad sobre el tratamiento posterior de los datos (una aplicación no fiel del principio de finalidad); la falta de una obligación general dirigida a las autoridades policiales de demostrar activamente su respeto de los principios de protección de datos; las débiles condiciones de verificación para la transferencia de datos a terceros países y, por último, la injustificada limitación de los poderes de las autoridades de control.

24. También se pronunciaron críticas a la reforma desde el Grupo de Trabajo, que lamentó que no se hubiese llegado a un único instrumento legislativo. El Grupo afirma que, por razones políticas, la Comisión optó por presentar una propuesta de Directiva específica sobre el sector de la policía y la justicia penal. En todo caso, añadió, que la nueva directiva no debía conducir a una disminución de los Estados miembros de sus respectivas normas de protección de datos establecidos para el sector de la policía y la justicia penal. El Grupo señala que el nuevo marco jurídico a adoptar debía estar alineado con otros acuerdos internacionales, como el Convenio n. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional, proponiendo insertar una referencia explícita al Convenio n. 108 y su protocolo adicional en el preámbulo del Reglamento y de la Directiva[1360].

[1358] El SEPD lamenta profundamente el contenido inadecuado de la Directiva específica sobre protección de datos en el ámbito de la policía y la justicia, afirmando: «*The Commission has not lived up to its promises to ensure a robust system for police and justice. These are areas where the use of personal information inevitably has an enormous impact on the lives of private individuals. It is difficult to understand why the Commission has excluded this area from what it intended to do, namely proposing a comprehensive legislative framework*». EDPS - Press Release (2012).

[1359] *Vid*. EDPS (2012), Opinion of the European Data Protection Supervisor on the data protection reform package, Brussels, 7 March 2012, págs. 4 y ss.

[1360] ARTICLE 29 DATA PROTECTION WORKING PARTY (2012b), Opinion 01/2012 on the data protection reform proposals, 00530/12/EN, WP 191, Adopted on 23 March 2012. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf; Opinion 08/2012 providing further input on the data protection reform discussions, 01574/12/EN, WP199, adopted on 05 October 2012; Opinion 01/2013 providing further

25. También el Comité Económico y Social Europeo, en su dictamen, aunque reconoció las ventajas y aspectos positivos necesariamente de la adopción de un reglamento en este delicado asunto, sin embargo, se planteaba la cuestión de la oportunidad de hacerlo. En particular, el Comité Económico y Social consideraba que la Comisión debía justificar mejor, especialmente a la luz del principio de subsidiariedad, las razones de hecho y de derecho que constituían la base para la adopción de un instrumento normativo altamente invasivo como es el reglamento, a fin de poner de relieve detalladamente las razones que llevaron a la Comisión a creer que fuese preferible a la adopción de una directiva. En igual medida, el Comité expresó su preocupación ante la posibilidad de sustraer a los Estados miembros cualquier prerrogativa de discreción con respecto a la aplicación de la legislación[1361].

26. Algunas críticas también se formularon por el Consejo de Europa en 2013, que publicó un informe sobre cómo los Estados miembros del Consejo de Europa han implementado las normas de la Recomendación R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros dirigida a regular la utilización de datos de carácter personal en el sector de la policía en sus legislaciones nacionales[1362]. Los resultados mostraron claras diferencias en el nivel de protección proporcionado en los Estados miembros. El hecho de que los Estados del Consejo de Europa afirmen haber implementado las reglas del Convenio n. 108 no significa que esos estándares se alcancen o que sean lo suficientemente altos. Esto respalda el reconocimiento de las instituciones de la Unión de la necesidad de emitir un "paquete de reformas" que adopte dos instrumentos, el RGPD y la Directiva, para uniformar la protección en la UE.

27. En cualquier caso, más allá de estas consideraciones técnicas, la totalidad de la doctrina, así como de las instituciones y de los órganos consultivos de la Unión Europea, acogieron de forma muy favorable la propuesta de Reglamento, considerando esta última

input into the discussions on the draft Police and Criminal Justice Data Protection Directive, 00379/13/EN, WP 201, Adopted on 26 February 2013.

[1361] *Vid*. DICTAMEN DEL COMITÉ ECONÓMICO Y SOCIAL EUROPEO sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)» COM(2012) 11 final - 2012/011 (COD), *Diario Oficial de la Unión Europea*, C 229, 31.7.2012, págs. 90–97. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012AE1303 [consulta: 15 de febrero de 2017].

[1362] *Vid*. Joseph A. CANNATACI and Mireille M. CARUANA (2013), *Report: Recommendation R (87) 15 – Twenty–five years down the line*, Council of Europe, 25th September, págs. 172. Disponible en Internet: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf [consulta: 15 de febrero de 2017].

como la solución preferida y más adecuada para reformar la legislación europea sobre la protección de datos personales.

2.2. La aprobación en primera lectura por el Parlamento Europeo bajo la fuerte oposición de los Estados

28. La propuesta de Reglamento, de conformidad con el procedimiento legislativo ordinario, fue objeto de un largo e intenso debate en el Parlamento Europeo. En esa sede, la comisión competente fue la Comisión LIBE. De hecho, el proyecto de Reglamento se presentó en la Comisión LIBE un proyecto de informe con algunas modificaciones al texto de la propuesta. En marzo de 2013, se publicaron las 3133 enmiendas al proyecto de informe elaborado por J. P. Albrecht ponente de la Comisión LIBE[1363]. Esto es lo que muestra el análisis de más de 11.000 páginas de documentos públicos y privados que han sido publicados por el sitio web *LobbyPlag.eu*[1364].

29. Con ocasión del Consejo JAI de 19 de julio de 2013, en Vilnus, los ministros de la Justicia francesa y alemana emitieron una declaración conjunta instando a la UE a emprender una acción rápida y ambiciosa sobre el paquete legislativo relativo a la protección de datos

[1363] La propuesta de reforma fue presentada a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) con 3.133 enmiendas. *Vid*. European Parliament - Committee on Civil Liberties, Justice and Home Affairs (2013a), AMENDMENTS (10) 2951 – 3133, Draft report Jan Philipp Albrecht (PE501.927v04-00), 2012/0011(COD), 8.3.2013; EUROPEAN COMMISSION - Memo (2013b), LIBE Committee vote backs new EU data protection rules, Brussels, 22 October 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-923_es.htm. En particular, se presentaron: 27 enmiendas de la Comisión de Empleo y Asuntos Sociales; 417 enmiendas registradas por la «*Comisión de Industria, Investigación y Energía*»; 226 de la «*Comisión de Mercado Interior y Protección del Consumidor*»; y 196 de la «*Comisión de Asuntos Jurídicos*», por un total de las enmiendas presentadas a la reforma sobre la protección de los datos personales de 3.999. Todas las enmiendas se pueden comprobar en el Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 22 de noviembre de 2013. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES#title2 [documentos consultados: 16 de febrero de 2017].

[1364] La asociación *LobbyPlag.eu* obtuvo alrededor de 11.000 páginas de documentos clasificados de la UE y una serie de "cables" diplomáticos alemanes clasificados sobre la reforma de protección de datos de la UE. Además de publicar muchos de los documentos, *LobbyPlag.eu* también muestra qué gobiernos nacionales están trabajando para reducir o aumentar las leyes de protección de datos en Europa. El objetivo de *LobbyPlag.eu* es transparentar los procedimientos democráticos complejos y opacos. La asociación se inició como un proyecto para seguir "copia y pega" la legislación de protección de datos en el Parlamento Europeo. Varios parlamentarios simplemente han copiado los cambios en las leyes de protección de datos de *Amazon*, *eBay*, la Cámara de Comercio Estadounidense, pero también de las ONG de privacidad. En consecuencia, esta "actividad legislativa" fue llamada "presionar y pegar". En 2013, *LobbyPlag.eu* rastreó los datos disponibles públicamente de 3.100 enmiendas presentadas por los miembros del Parlamento Europeo, lo que permitió a las personas y a los periodistas averiguar fácilmente qué proponen sus representantes. Sitio web de la asociación: *www.lobbyplag.eu*.

personales[1365]. España, Países Bajos, Austria, Italia y Polonia expresaron su apoyo a la propuesta franco-alemana. En cuanto a la propuesta de Directiva, su contenido amplía el alcance de la aplicación de la Decisión Marco 2008/977/JAI[1366]: ya no sólo se aplica a aquellas actividades transfronterizas de intercambio de datos, sino que también cubriría el tratamiento de datos en el ámbito estrictamente nacional. Sin embargo, algunos Estados miembros se opusieron a esta novedad, argumentando que la regulación del tratamiento de datos a nivel nacional podría ir en contra del principio europeo de subsidiariedad (Suecia), y consideraban que la Decisión Marco 2008/977/JAI era suficiente[1367] (Alemania, Dinamarca y Reino Unido). Otros expresaron sus dudas sobre la viabilidad de la propuesta puesto que pretendía armonizar las leyes de protección de datos en el ámbito policial[1368].

30. Asimismo, la opción de una regulación que también cubriese el ámbito penal era aparentemente inaceptable para la mayoría de los Estados miembros, por lo que, finalmente, se decidió adoptar una directiva con los mismos planteamientos que el reglamento, pero con las limitaciones y excepciones pertinentes, y dejando más espacio para la aplicación a nivel

[1365] «EU justice ministers agreed to seek better data protection», en *Lithuanian Presidency of the EU Council 2013*, 19 July 2013. Disponible en Internet: http://www.eu2013.lt/en/news/pressreleases/eu-justice-ministers-agreed-to-seek-better-data-protection- [consulta: 16 de febrero de 2017].

[1366] Uno de los temas más polémicos tuvo que ver con la propuesta de Directiva que se filtró en noviembre de 2011, dos meses antes de que se publicara la versión de propuesta oficial por la Comisión. En aquel primer borrador aparecían mayores garantías de protección de datos que las que finalmente se incluyeron en la versión final de propuesta. Por ejemplo, la propuesta oficial no contiene mención alguna de las llamadas evaluaciones de impacto de protección de datos, que sí aparecían en el borrador filtrado. En Cristina BLASI CASAGRAN (2015: 139).

[1367] PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 11624/1/13, REV 1, Brussels, 2 October 2013, pág. 2. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-11624-2013-REV-1/en/pdf [consulta: 17 de febrero de 2017]. El Reino Unido consideró que las normas mínimas establecidas en la Decisión Marco eran suficientes y apropiadas para la protección de los derechos fundamentales en el contexto de la cooperación policial y judicial. El Reino Unido considera que la propuesta de Directiva no debe aplicarse a la transformación nacional, mientras que Dinamarca era escéptica al incluir el tratamiento estrictamente nacional, debido al principio de subsidiariedad. Para Alemania los estándares mínimos eran mejores que la armonización total.

[1368] Algunas delegaciones (Alemania, Francia y Hungría) se refirieron a las dificultades relacionadas con las superposiciones parciales entre la propuesta de Reglamento y Directiva. Alemania reconoció que esta superposición no era nueva, pero que las dificultades vinculadas se verían reforzadas por el alcance más amplio y la naturaleza menos flexible de la Directiva en comparación con la Decisión Marco. Hungría habría preferido un único instrumento jurídico (una Directiva), ya que tanto el artículo 8 de la CDFUE como el artículo 16 del TFUE exigen un marco global aplicable horizontalmente. También véase PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters I-IV, 14901/2/13, REV 2, Brussels, 30 October 2013, pág. 4. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-14901-2013-REV-2/en/pdf [consulta: 17 de febrero de 2017].

nacional. Así, el 21 de octubre de 2013[1369], después de una intensa actividad de "*lobbying*"[1370], la Comisión LIBE adoptó (informe depositado el 22 de noviembre de 2013)[1371], la propuesta de Reglamento con 51 votos a favor, 1 en contra y 3 abstenciones, y la propuesta de Directiva con 47 votos a favor, 4 en contra y 1 abstención.

31. Previa a la aprobación, el Parlamento Europeo, en su Resolución de 4 de julio de 2013[1372], había expresado su «*profunda preocupación*»[1373] por los programas de vigilancia sistemáticos de la Agencia Nacional de Seguridad de los EE.UU., responsable de haber vigilado, filtrado, y registrado datos de empresas telefónicas y tecnológicas (como *Verizon*, *Microsoft* y *Google*), haciendo uso de la posibilidad, prevista por la *Patriot Act* (Sección 215) de EE.UU., para obtener acceso directo a la información sobre la base de una orden judicial secreta, por exigencias de la lucha contra el terrorismo. La Resolución del Parlamento no tiene precedentes y hace un llamamiento a los aliados atlánticos a interrumpir y reflexionar las leyes y los programas de vigilancia que afectan no sólo a la soberanía de los Estados europeos, sino también a los derechos fundamentales de sus ciudadanos. También se piden modificaciones a los Estados miembros, así como la posible suspensión «*de los acuerdos sobre el registro de nombres de los pasajeros (PNR) y sobre el Programa*

[1369] EUROPEAN PARLIAMENT - Press Releases (2013), Civil Liberties MEPs pave the way for stronger data protection in the EU, 21-10-2013.

[1370] Kevin J. O'BRIEN (2013), «Silicon Valley Companies Lobbying Against Europe's Privacy Proposals», en *The New York Times*, Jan. 25. Disponible en Internet: http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=0; Nikolaj NIELSEN (2013), «MEPs copy-pasting amendments from US lobbyists», en *EUobserver*, Brussels, 12 Feb. Disponible en Internet: https://euobserver.com/justice/119028; Rosario G. GÓMEZ, María R. SAHUQUILLO (2013), «Los colosos de la Red se alían contra la nueva ley de privacidad de la UE», en *El País*, Madrid, 24 Feb. Disponible en Internet: http://sociedad.elpais.com/sociedad/2013/02/24/actualidad/1361744770_097775.html [documentos consultados: 17 de febrero de 2017]; y Nikolaj NIELSEN (2016).

[1371] Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 22 de noviembre de 2013.

[1372] Resolución del Parlamento Europeo, de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE (2013/2682(RSP)), Jueves 4 de julio de 2013 - Estrasburgo. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//ES [consulta: 18 de febrero de 2017]. Recordamos que la Resolución es la consecuencia de lo que había salido a la luz con el estallido del escándalo "*Datagate*".

[1373] Apartado 9 de la Resolución del Parlamento Europeo, de 4 de julio de 2013: «*Expresa su profunda preocupación ante las revelaciones de supuestos programas de vigilancia aplicados por Estados miembros, con la ayuda de la Agencia Nacional de Seguridad de los EE.UU. (NSA) o unilateralmente; pide a los Estados miembros que examinen la compatibilidad de estos programas con el Derecho primario y secundario de la UE, en particular el artículo 16 del TFUE relativo a la protección de datos, y con las obligaciones en materia de derechos fundamentales de la UE que se derivan del CEDH y de las tradiciones constitucionales comunes de los Estados miembros*».

de Seguimiento de la Financiación del Terrorismo (TFTP)»[1374]. La Resolución también disponía que la Comisión LIBE realizase una «*investigación exhaustiva sobre este asunto en colaboración con los Parlamentos nacionales y el grupo de expertos UE-EE.UU. creado por la Comisión*»[1375]. De hecho, la Comisión parlamentaria LIBE, planteó en varias ocasiones, en el desarrollo de la investigación encargada por el Parlamento bajo el título "*Electronic Mass Surveillance of EU Citizens*"[1376], la necesidad de adoptar medidas para evitar el riesgo de una violación de la protección de datos personales de los ciudadanos europeos aún mayor que la perpetrada por la *NSA*[1377].

32. A lo largo del desarrollo de este largo proceso, y con ocasión del "Día de la Protección de Datos 2014", que se celebra el 28 de enero de cada año, la vicepresidenta de la Comisión Viviane Reding, propuso un nuevo "pacto europeo en materia de protección de datos", basado en ocho principios, entre los que se pueden destacar los siguientes: que «*la recogida de datos debería ser específica y limitarse de forma proporcional a los objetivos que se hayan fijado. La vigilancia general de los datos de las comunicaciones electrónicas no es aceptable*»; que «*las leyes han de ser claras y deben actualizarse. Los Estados no deberían basarse en normas desfasadas,* (…) *para crear el marco de los programas modernos de vigilancia*»; y que «*la seguridad nacional debería invocarse con mesura: debe ser la excepción y no la regla*»[1378].

[1374] Apartado 4 de la Resolución del Parlamento Europeo, de 4 de julio de 2013. La suspensión de dichos acuerdos por parte de la Comisión Europea en la Resolución no tiene valor vinculante de la misma y deja espacio a futuras consideraciones políticas sobre esta oportunidad.

[1375] Apartado 16 de la Resolución del Parlamento Europeo, de 4 de julio de 2013.

[1376] EUROPEAN PARLIAMENT - Committee on Civil Liberties, Justice and Home Affairs (2013b), LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - Final programme, Brussels, 14 October 2013. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131014_1500.htm# [consulta: 18 de febrero de 2017].

[1377] En palabras de Caspar Bowden, autor de la investigación "*The U.S. surveillance programmes and their impact on EU citizens' fundamental rights*", que plantea con claridad las razones de la preocupación europea. *Cfr*. Caspar BOWDEN (2013), *The U.S. surveillance programmes and their impact on EU citizens' fundamental rights*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, September, págs. 37. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf y Didier BIGO, Sergio CARRERA, Nicholas HERNANZ, *et ál*. (2013), *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, October, pág. 9. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf [consultados: 18 de febrero de 2017].

[1378] COMISIÓN EUROPEA - Comunicado de prensa (2014a), Día de la Protección de Datos 2014: la vicepresidenta Reding aboga por un nuevo pacto europeo en materia de protección de datos, Bruselas, 28 de enero de 2014. Disponible en Internet: http://europa.eu/rapid/press-release_IP-14-70_es.htm [consulta: 19 de febrero de 2017]. Por último, la vicepresidenta Reding lanza un mensaje a los estadounidenses: «*las normas de protección de datos deben aplicarse independientemente de la nacionalidad de la persona de que se trate.*

33. Mientras tanto, la propuesta de Reglamento también fue discutida por el Consejo de la Unión Europea, en particular por el Consejo de Justicia y Asuntos de Interior, reunido en Bruselas el 3 y 4 de marzo[1379]. Pero el paso más importante tuvo lugar el 12 de marzo de 2014 (sesión de 11 a 14 marzo)[1380], cuando el Parlamento Europeo, en sesión plenaria, adoptó su posición en primera lectura sobre la propuesta de Reglamento y la propuesta de Directiva, como base de las negociaciones entre las instituciones. El Parlamento respaldó la configuración original apoyando las dos propuestas como parte de un "paquete" de normas de forma conjunta[1381]. Por esta razón, muchas enmiendas a la propuesta de Directiva sobre el tratamiento de datos personales en las actividades policiales y judiciales tienen por objeto garantizar la coherencia con las disposiciones del Reglamento propuesto, por ejemplo, en comparación con las definiciones, los poderes de las autoridades de control y su previa consulta o para ciertos elementos. En fin, el texto sobre la propuesta de Reglamento resultó aprobado de manera aplastante con 621 votos a favor, 10 en contra y 22 abstenciones y la propuesta de Directiva con 371 votos a favor, 276 en contra y 30 abstenciones. Este paso representó un importante impulso, formal y sustancial, en el desarrollo de la tramitación legislativa.

34. Sin embargo, el proceso legislativo de las propuestas fue inmediatamente frenado por los fuertes enfrentamientos entre las instituciones y los Estados miembros, que se acentuaron después de la primera lectura del Parlamento Europeo: aunque se aprobaron los textos

Aplicar normas diferentes a los nacionales y a los no nacionales no tiene ningún sentido teniendo en cuenta el carácter abierto de Internet».

[1379] COUNCIL OF THE EUROPEAN UNION - Press Release (2014), 3298th Council meeting, Justice and Home Affairs, Brussels, 3 and 4 March 2014, 7095/14. Se reunió el Consejo JAI para discutir el ámbito de aplicación territorial, la transferencia internacional de datos, los datos con seudónimo, la portabilidad de datos, y las obligaciones del responsable y encargado de procesamiento de datos y elaboración de perfiles.

[1380] RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura), Miércoles 12 de marzo de 2014 - Estrasburgo. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES [consulta: 19 de febrero de 2017].

[1381] PARLAMENTO EUROPEO - Notas de prensa (2014b), La Eurocámara refuerza la protección de datos de los europeos en la era digital, Sesión plenaria, 12-03-2014. Disponible en Internet: http://www.europarl.europa.eu/news/es/news-room/content/20140307IPR38204/html/La-Euroc%C3%A1mara-refuerza-la-protecci%C3%B3n-de-datos-de-los-europeos-en-la-era-digital [consulta: 19 de febrero de 2017]. Durante el debate sobre el paquete legislativo en su conjunto, los dos ponentes (Jan-Philipp Albrecht y Dimitrios Droutsas) expresaron el deseo de mantener un enfoque global, instando al Parlamento a aprobar las dos propuestas para alinear un solo instrumento europeo de tratamiento de datos personales. Los oradores también subrayaron la irresponsabilidad de un nuevo aplazamiento, y se les pidió que, dos años después de la propuesta de la Comisión, el Consejo defina una posición clara y encuentre lo más pronto posible un acuerdo sobre una impostación general. También se expresó frustración por el comportamiento de algunos Estados miembros que ha impedido que se pueda aprobar el paquete de reformas en materia de protección de datos a finales de este término parlamentario.

propuestos por la Comisión, el Parlamento introdujo enmiendas desequilibrando la propuesta de Reglamento hacia una mayor garantía del derecho a la protección de datos más que hacia el buen funcionamiento del mercado interior[1382]. De hecho, la posición del Parlamento también fue influenciada por la necesidad de dar respuestas contundentes a las actividades de vigilancia masivas ligadas a "*Datagate*" conocidas desde junio de 2013. La votación en seno el Parlamento impulsó al fortalecimiento de los derechos de los interesados, e introdujo fuertes sanciones para las empresas que violasen los principios de protección de datos personales. En comparación con la Directiva 95/46/CE, la propuesta de Reglamento reorganizaba el contenido, ampliándolo considerablemente: se pasa de siete capítulos y 34 artículos de la Directiva a 91 artículos divididos en once capítulos contenidos en la propuesta de Reglamento[1383].

2.3. Adopción en primera lectura en el Consejo de la UE y adopción de una "orientación general" sobre el Reglamento

35. Como se ha indicado, de acuerdo con el procedimiento de legislativo ordinario, el Parlamento presentó su posición en primera lectura al Consejo de la Unión Europea. Los trabajos preliminares sobre la primera lectura del Consejo van adelante en paralelo con los

[1382] RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014. En realidad, el Parlamento europeo introdujo modificaciones en las normas relativas a la participación de las empresas (motor de búsqueda, *social network* o proveedor "*cloud*"): estos sujetos, bajo las nuevas normas, deberían pedir una autorización preventiva a la autoridad nacional de protección de los datos antes de divulgar los datos personales de un ciudadano de la Unión en un Estado no miembro; la empresa también debería informar a la persona interesada de la solicitud. Además, el texto enmendado de la reforma introdujo sanciones en forma de multas de hasta € 100 millones o hasta 5% del volumen de negocios anual mundial (se aplicaría el castigo más severo de los dos), donde la Comisión proponía inicialmente multas de hasta 1 millón de euro o hasta un 2% del volumen de negocios anual mundial.

[1383] Las principales modificaciones, en lo que, respecta a la Directiva de 1995, se pueden resumir de la siguiente manera: la disposición de que el consentimiento para el uso de sus datos personales debe ser clara y explícita, lo que excluye la posibilidad de un consentimiento tácito; la introducción de garantías en el caso de los datos personales que se relacionan con los niños; el fortalecimiento del derecho a la supresión de los datos personales, cuando no hay razones que permitieron el uso, y la introducción del "derecho al olvido"; la introducción del derecho a la portabilidad de los datos (a través de un procedimiento simplificado), es decir, el derecho a transferir sus datos entre diferentes sistemas electrónicos sin que el controlador pueda impedirlo; la introducción de disposiciones que especifican en términos más precisos el derecho a no ser sometido a "elaboración de perfiles" ("*profiling*"); mayor responsabilidad y la obligación de la documentación para el controlador de los datos; obligación de que el procesador de la notificación y divulgación de todas las violaciones de los datos personales; la institución de la figura obligatoria del responsable de la protección de los datos personales para el sector público y las empresas que tengan al menos 250 dependientes; las disposiciones para regular la transferencia de datos personales a países terceros u organizaciones internacionales: la propuesta de Reglamento establece que la transferencia debe estar sujeta a la adopción previa de la Comisión, una decisión que pone a prueba el carácter adecuado del nivel de protección ofrecida por el Estado destinatario de las información; también se prevé que, en ausencia de una decisión de la Comisión, se pueda proceder a la transferencia, siempre y cuando se averigüen ciertas circunstancias que en la Propuesta están debidamente indicadas; la asignación a la autoridad de control del poder de imponer sanciones administrativas en caso de incumplimiento de las obligaciones; y la instrodución del Comité Europeo para la Protección de los Datos, compuesta por los responsables de las autoridades de control de los Estados miembros y del SEPD.

del Parlamento, pero el Consejo puede proceder a su primera lectura formalmente sólo después de recibir la posición que el Parlamento expresó en primera lectura. El Consejo de Justicia y Asuntos de Interior (JAI) es responsable de lo que se refiere al ámbito de la protección de datos. El Consejo puede aceptar la posición expresada por el Parlamento en primera lectura o puede aprobar su propia versión modificada (respecto a la propuesta de la Comisión Europea), expresándose con su primera lectura. Sin embargo, antes de expresar oficialmente su posición con un texto aprobado en la primera lectura, el Consejo puede adoptar una "orientación general", que sirve para dar una idea al Parlamento sobre la posición del Consejo con respecto de la propuesta de la Comisión. Esta "orientación general" se utiliza para acelerar el procedimiento legislativo y facilitar el logro de un acuerdo entre las instituciones a través de reuniones de interrelación llamadas "diálogos tripartitos".

36. En cuanto al Consejo, los Estados miembros todavía no habían llegado a un enfoque común en general, levantando críticas con especial referencia a la propuesta de RGPD. Unas de las cuestiones más relevantes debatidas por el Consejo, es la relativa al tema de la introducción de la "ventanilla única"[1384] o una única autoridad capaz de analizar casos transnacionales y asegurar la aplicación coherente y uniforme de la legislación, reduciendo los gravámenes administrativos para las empresas que operan en el comercio internacional[1385]. En el Consejo de Justicia y Asuntos de Interior celebrado los días 4 y 5 de diciembre de 2014, los ministros aprobaron una "orientación general" parcial sobre la

[1384] El 6 de junio de 2014, se reunió en Luxemburgo el Consejo JAI, en el que los ministros llegaron a una orientación general parcial sobre el quinto Capítulo de la propuesta de Reglamento. Además, hubo un debate sobre el mecanismo de "*one-stop-shop*" (mecanismo de ventanilla única), pero sin llegar a un acuerdo. En esta ocasión, la vicepresidenta de la Comisión Europea Viviane Reding, subrayó la importancia de concluir en tiempos breves la reforma de la normativa europea sobre la protección de los datos personales, esencial para la realización del mercado único digital. Además, la vicepresidenta se mostró a favor del texto, tanto en términos del ámbito de aplicación territorial tanto de la transferencia internacional de datos. *Cfr*. CONSEJO DE LA UNIÓN EUROPEA (2014a), Consejo de Justicia y Asuntos de Interior, 05-6.6.2014, Sesión n. 3319, Luxemburgo, 5.6.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/06/05-06/ [consulta: 22 de febrero de 2017].

[1385] El 9 y 10 de octubre de 2014, se reunió en Luxemburgo el Consejo de Justicia y Asuntos de Interior. Los ministros de la UE llegaron a una orientación general parcial sobre el Capítulo IV de la propuesta de Reglamento, basada sobre las obligaciones del responsable y el encargado del tratatamiento de datos y sobre la necesidad de introducir una aproximación basada sobre el riesgo. El Capítulo IV es sin duda una de las claves de la propuesta de Reglamento, ya que introduce el enfoque basado sobre el riesgo, y es un criterio válido para la definición de las obligaciones de privacidad. De hecho, permite evitar la previsión de gravámenes no justificada por concretas exigencias de tutela de los datos. CONSEJO DE LA UNIÓN EUROPEA (2014b), Consejo de Justicia y Asuntos de Interior, 09-10.10.2014, Sesión n. 3336, Luxemburgo, 9.10.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/10/09-10/ [consulta: 22 de febrero de 2017]. El Consejo celebró también un debate político sobre el "derecho al olvido", siguiendo así la sentencia del TJUE de 13 de mayo de mismo año en el caso de *Google Spain*. Mientras que algunos ministros de la UE están de acuerdo en construir una jurisdicción pública capaz de afrontar la cuestión del derecho al olvido y no dejar la interpretación a las entidades privadas que operan en las plataformas en línea, por el otro lado, muchos Estados miembros (Reino Unido, Luxemburgo, Bélgica, Dinamarca, Países Bajos, Eslovenia y Rumania), insistieron en la necesidad de encontrar una solución "en cada caso".

propuesta de RGPD[1386]. La "orientación general" parcial cubría artículos fundamentales para la cuestión del sector público, y también incluía disposiciones relativas a situaciones específicas de tratamiento de datos[1387]. En la misma reunión, la Presidencia italiana informó al Consejo sobre el estado de los trabajos de la Directiva relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales a efectos policiales y judiciales. El 12 y 13 de marzo de 2015, se celebró en Bruselas el primer Consejo de Justicia y Asuntos de Interior bajo la Presidencia de Letonia[1388], que alcanzó una "orientación general" parcial sobre el Reglamento sobre protección de datos, con la intención de que nada quedase acordado hasta que todo hubiese sido acordado. El texto refrendado incluye el mecanismo de ventanilla única[1389] y los principios relativos al tratamiento de datos personales[1390].

37. El 15 de junio de 2015, los ministros de Justicia y Asuntos de Interior lograron una "orientación general" sobre el RGPD[1391]. Se trataba, según el comunicado conclusivo, de

[1386] CONSEJO DE LA UNIÓN EUROPEA (2014c), Consejo de Justicia y Asuntos de Interior, 4-5.12.2014, Sesión n. 3354, Bruselas, 4-5.12.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/12/04-05/ [consulta: 22 de febrero de 2017]. El Consejo celebró también un debate político sobre el mecanismo de "ventanilla única", basada en una propuesta presentada por la Presidencia italiana, que tiene en cuenta la necesidad, expresada también por el Servicio Jurídico del Consejo, para mejorar la proximidad entre los individuos y las autoridades de vigilancia locales, en los procesos de decisión.

[1387] PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), 15656/1/14, REV 1, Brussels, 28 November 2014. Disponible en Internet: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015656%202014%20REV%201 [consulta: 22 de febrero de 2017].

[1388] CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015a), Protección de datos: El Consejo llega a un acuerdo sobre los principios generales y el mecanismo de ventanilla única, 114/15, 13.3.2015. Disponible en Internet: http://www2.consilium.europa.eu/es/press/press-releases/2015/03/13/data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/ [consulta: 22 de febrero de 2017]. El Consejo también trató la aplicación de las medidas en materia de lucha contra el terrorismo: aplicación reforzada del Marco de Schengen, combatiendo la radicalización en internet mediante la creación de discapacidades «*de notificación de contenidos de internet*», luchando «*contra el tráfico ilícito de armas de fuego*» e intensificando el «*intercambio de información y la cooperación operativa*».

[1389] PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - The one-stop-shop mechanism, 2012/0011 (COD), 6833/15, Brussels, 9 March 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf#http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf%20 [consulta: 23 de febrero de 2017].

[1390] PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Chapter II, 2012/0011 (COD), 6834/15, Brussels, 9 March 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6834-2015-INIT/en/pdf [consulta: 23 de febrero de 2017].

[1391] Una orientación general significa que el Consejo llega a un acuerdo político sobre cuya base puede ya iniciar las negociaciones con el Parlamento Europeo con el fin de llegar a un acuerdo general sobre unas nuevas normas de protección de datos en la UE. *Vid*. CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa

una reglamentación que «*reforzará los derechos individuales de nuestros ciudadanos y garantizará un nivel de protección elevado*». Las nuevas reglas, que debían sustituir a las aplicadas por los Estados individuales, incluían el consentimiento explícito a todo lo relacionado con los datos personales, un acceso simplificado a los mismos, una información clara y comprensible sobre el uso que se haga de ello, el "derecho al olvido" (cancelación de los datos personales)[1392], una portabilidad que facilite la transferencia de datos personales de un proveedor de servicio a otro (como se hace para la telefonía) y la limitación de la "elaboración de perfiles" (tratamiento automatizado de datos de carácter personal para determinar aspectos personales de una persona física)[1393].

38. Después de tres años de negociaciones, el Consejo JAI llegó a un acuerdo a pesar de la oposición de Eslovenia y Austria y algunas reservas expresadas por Hungría y Polonia. En general, todos los Estados miembros habían expresado diversas preocupaciones en el debate, con especial referencia al capítulo de "reutilización" de los datos para fines distintos de los inicialmente aceptados por aquellos cuyos datos sean objeto de tratamiento. Este es el caso de Polonia, Austria, Italia, Chipre, Bélgica y España. Francia, Hungría y Chipre insistieron en el fortalecimiento del derecho al olvido. Gran Bretaña y Polonia expresaron reservas sobre el mecanismo de la "ventanilla única", mientras que Malta sobre el tema de la "portabilidad" de los datos[1394].

2.4. Los diálogos tripartitos y la aprobación de la "orientación general" sobre la Directiva

39. Basándose en el acuerdo de 15 de junio de 2015, el Consejo inició las negociaciones con el Parlamento Europeo (recordemos, diálogos tripartitos)[1395], que involucraban a las tres instituciones principales de la UE (Parlamento, Consejo y Comisión Europea), con el apoyo

(2015b), Protección de datos: el Consejo acuerda una orientación general, 450/15, 15.6.2015; y COMISIÓN EUROPEA - Comunicado de prensa (2015a).

[1392] Cuando el ciudadano no quiere que los datos que lo conciernen sean tratados más y no existan motivos legítimos para conservarlos, el responsable del trato tiene que borrarlos, o bien demostrar que todavía son necesarios o pertinentes.

[1393] Las normas establecían una "ventanilla única" para las empresas y los ciudadanos: el hecho de tener que interactuar con una única autoridad de supervisión (en lugar de 28) debía facilitar y hacer menos costoso para las empresas operar en toda la UE. También si un usuario considerase violado su derecho a la privacidad le permitiría recurrir directamente a los tribunales de su país y en su lengua.

[1394] PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 2012/0011 (COD), 9565/15, Brussels, 11 June 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [consulta: 24 de febrero de 2017].

[1395] «Procedimiento legislativo ordinario. Fase 2: Primera lectura», en *Consejo de la Unión Europea*. Disponible en Internet: http://www.consilium.europa.eu/es/council-eu/decision-making/ordinary-legislative-procedure/first-reading/ [consulta: 24 de febrero de 2017].

del SEPD que desempeña un papel importante en sede consultiva[1396], con el objetivo de alcanzar en un breve período un acuerdo sobre el nuevo RGPD y la Directiva en material de tratamiento policial y penal.

40. Al mismo tiempo, con referencia al nuevo marco establecido por el "paquete de reformas", el Grupo de Trabajo[1397] intervino varias veces, proporcionando su apoyo técnico en las diferentes etapas del proceso de regulación. El Grupo se dirigió a las instituciones políticas que participaban en la reforma, llamando la atención sobre una serie de prioridades y objetivos a considerar en el diseño de nuevas herramientas[1398]. En este sentido, la Comisión Europea, al presentar en 2012 su propuesta de Reglamento, adoptó una importante decisión de política pública ya que se trataba de ir más allá del cumplimiento, impulsando de manera decidida un marco normativo modernizado que no supusiera un coste adicional para quienes tratan datos personales. Se trata, por tanto, de una política pública destinada a proteger al titular de los datos personales a través de obligaciones y garantías, ya que, a través de dicho principio, y también del "principio de protección de datos por defecto", se busca conseguir el objetivo de que los productos y servicios que se ofrezcan a aquellos incluyan salvaguardias desde la fase más temprana posible de diseño. Según el Grupo era necesario, en primer lugar,

[1396] «*In 2016, we will continue to work closely with the European Commission, the Council and the European Parliament in order to ensure that our advice is as timely and relevant as possible. By making our Priorities public, we hope to help the relevant Commission services to better identify those initiatives on which the EDPS recommends an informal consultation at an early stage, as per our long-standing agreement*». Así se pronunció en una nota de prensa el SEPD, Giovanni Buttarelli, sobre la colaboración entre el Supervisor y las instituciones europeas. En EDPS - Press Release (2016), Priorities for 2016: The EDPS as an advisor to the EU Institutions, EDPS/2016/02, Brussels, 7 January 2016.

[1397] El Grupo continuó proporcionando orientación y opiniones adoptadas sobre la base de los temas estratégicos descritos en el programa de trabajo para el período 2014-2015 adoptado el 3 de diciembre 2013. Vid. GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS (2013), Programa de trabajo 2014 - 2015, 02124/13/ES, WP 210, Adoptado el 3 de diciembre de 2013. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_es.pdf [consulta: 24 de febrero de 2017]. El Grupo aprovechó todas las oportunidades posibles para ayudar a crear un nuevo marco legal, más coherente, garantista y eficaz, mediante el envío de sus observaciones a las tres instituciones de la UE que participaban en los diálogos tripartitos - y para aclarar los efectos sobre el marco regulatorio actual de las sentencias más importantes adoptadas por el TJUE en la conservación de datos de tráfico (asunto *Digital Rights Ireland*), ley aplicable (asuntos *Google Spain* y *Weltimmo*) y transferencias de datos en el extranjero (asunto *Schrems*)-.

[1398] Cartas de 17 de junio de 2015 del Grupo de Trabajo enviadas a las instituciones europeas: ARTICLE 29 DATA PROTECTION WORKING PARTY (2015g), Ms Ilze Juhansone, Ambassador Extraordinary and Plenipotentiary, Permanent Representative to the European Union. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjuhansone_en.pdf; Mr Jan Philipp Albrecht, Vice Chair Committee on Civil Liberties, Justice and Home Affairs. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_mralbrecht_en.pdf; Ms Věra Jourová, Commissioner for Justice, Consumers and Gender Equality European Commission. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjourova_en.pdf [documentos consultados: 25 de febrero de 2017].

que el paquete de reformas permitiera mantener un alto nivel de protección hasta ahora garantizado por la Directiva 95/46/CE y que no representase de ninguna manera una reducción del sistema de protección existente. Sobre las relaciones entre los dos instrumentos legislativos en cuestión, reglamento y directiva, según el Grupo, era necesario la plena concordancia entre los dos marcos reguladores, y que la propuesta de Directiva fuese una excepción a los principios del Reglamento, que estaría limitado exclusivamente al ámbito de la prevención y persecución de delitos, sin extenderse a otras actividades de las autoridades públicas[1399].

41. Con ocasión del acuerdo alcanzado por el Consejo, la reunión para iniciar las negociaciones tripartitas ("*kick-off trilogue meeting*") se llevó a cabo el 24 de junio 2015[1400]. El 27 de julio 2015 el SEPD envió una recomendación a los órganos legislativos de la Unión interesados en la negociación del nuevo RGPD. El SEPD afirmó que los principios vigentes en el paquete de reformas «*deben aplicarse de manera coherente, dinámica e innovadora, de manera que sean eficaces para el ciudadano en la práctica. La reforma tiene que ser exhaustiva, de ahí el compromiso con el desarrollo de un paquete, aunque, dado que es probable que el tratamiento de datos se aborde en instrumentos jurídicos distintos, habrá de establecerse con claridad su ámbito de aplicación exacto y el modo en que aquellos interactúan, de manera que no existan lagunas que permitan vulnerar las*

[1399] Con referencia a los principios fundamentales de la reforma, el Grupo señaló que el concepto de dato personal tuvo que ser lo suficientemente amplio para satisfacer los requisitos de protección resultantes de las nuevas tecnologías. También se necesitaba una estricta observancia del principio de finalidad –que no admite tratamiento incompatible con los fines legítimos del tratamiento original– y que fueran garantizadas las herramientas necesarias para asegurar un fácil ejercicio de los derechos de parte de los interesados, en un marco reglamentario basado en un nuevo gobierno basado en la proximidad a las personas y la eficiencia al mundo empresarial. Con este fin, el Grupo ofreció algunas sugerencias técnicas en el desarrollo de las negociaciones tripartitas en el documento anexo a las letras anteriores. *Cfr*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2015b), Annex to the letters: Core topics in view of the trilogue, 17 June 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf. El Grupo, con una carta de 25 de septiembre de 2015 dirigida a las tres instituciones europeas, proporcionó varias observaciones acerca de la estructura interna del Comité Europeo de Protección de Datos para asegurar que este órgano contase con una estructura flexible y equilibrada, capaz de aumentar la red descentralizada de las autoridades de protección de datos y para proporcionar una coordinación eficiente y estable. Vid. ARTICLE 29 DATA PROTECTION WORKING PARTY (2015c), Propositions regarding the European Data Protection Board Internal Structure, 15 September 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150925_edpb_internal_structure.pdf [documentos consultados: 26 de febrero de 2017].

[1400] EUROPEAN COMMISSION - Statement (2015), Remarks by Commissioner Jourová after the launch of the Data protection regulation trilogue, Brussels, 24 June 2015. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm; PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation for trilogue, 2012/0011 (COD), 9985/1/15, REV 1, Brussels, 11 June 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-9985-2015-REV-1/en/pdf [consulta: 26 de febrero de 2017].

salvaguardias»[1401]. El SEPD, para estimular la reanudación de los trabajos, formuló observaciones específicas respecto al texto del Reglamento en elaboración y puso a disposición un documento en el que se comparaba el texto original de la propuesta de la Comisión, el texto modificado por el Parlamento Europeo, los cambios introducidos por el Consejo y otras recomendaciones del mismo SEPD[1402].

42. El 9 de octubre de 2015, el Consejo de la UE, finalmente, aprobó la "orientación general" ("*general approach*") sobre la Directiva relativa a la protección de datos personales con fines de cooperación policial y judicial en materia penal. El objetivo del proyecto de Directiva era «*garantizar un alto nivel de protección de los datos personales*» y «*facilitar el intercambio de datos personales entre fuerzas y cuerpos de seguridad dentro de la Unión Europea*»[1403]. La Directiva, se aplicaría a los datos transfronterizos, tanto al trato de las autoridades judiciales y las autoridades policiales a nivel nacional, mientras que el marco legal vigente de las normas europeas debía aplicarse únicamente a la transferencia transfronteriza. Este elemento ralentizó y a veces obstaculizó el desarrollo de la cooperación judicial entre Estados miembros. En particular, en Europa se sentía la necesidad de facilitar el intercambio de datos personales entre los servicios judiciales y policiales de los Estados miembros, reforzando aquellos aspectos descuidados por las intervenciones reguladoras anteriores en esta área.

43. La iniciativa también refleja la conciencia de la importancia de facilitar el intercambio de datos personales con el fin de prevenir y combatir el terrorismo, particularmente en un contexto de preocupante fragmentación y difusión de las células terroristas. La intervención reguladora, además, tiene como objetivo el fortalecimiento de la «*confianza mutua entre las autoridades judiciales de los distintos países*»[1404]. Se mantiene

[1401] DICTAMEN 3/2015. La gran oportunidad de Europa. Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos, Bruselas, 28 de julio de 2015, pág. 7. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_ES.pdf [consulta: 26 de febrero de 2017].

[1402] EDPS (2015a), Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations, 27 July 2015, págs. 520. La autoridad también promovió el lanzamiento de una aplicación para dispositivos móviles (*app*) para una fácil comparativa de los diversos textos. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package.

[1403] CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015c), Protección de datos con fines de cooperación policial y judicial en materia penal: el Consejo, preparado para las conversaciones con el Parlamento Europeo, 712/15, 09.10.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/10/09-data-protection/ [consulta: 27 de febrero de 2017].

[1404] CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015c).

en vigor el sistema de las autoridades nacionales de supervisión mientras que las nuevas reglas se aplican también a los terceros países y organizaciones internacionales.

44. Con la aprobación de la "orientación general" sobre la Directiva se inició un procedimiento de conciliación entre el Parlamento, el Consejo y la Comisión Europea. De este modo, el 15 de diciembre de 2015, después de casi cuatro años de su propuesta de reforma, la Comisión llegó a un acuerdo sobre la reforma de la protección de datos[1405] con el Parlamento Europeo y el Consejo, tras las negociaciones finales entre las tres instituciones. A tal propósito, Věra Jourová, la nueva Comisaria de Justicia, Consumidores e Igualdad de Género, sobre la importancia de la reforma, declaró que «*unas normas armonizadas de protección de datos para las autoridades policiales y judiciales facilitarán la cooperación en este ámbito entre los Estados miembros sobre la base de la confianza mutua* (…)». En una reunión extraordinaria, la Comisión (LIBE) aprobó el texto acordado en los diálogos tripartitos el 17 de diciembre de 2015.

45. Sobre este acuerdo, cabe señalar que el Grupo de Trabajo, en su opinión 3/2015, expresó ciertas críticas acerca de algunos temas e hizo sugerencias sobre el proyecto de Directiva europea sobre protección de datos utilizada con fines judiciales y policiales[1406]. Esta opinión del Grupo de Trabajo, en lo que respecta al nivel mínimo de protección de los datos personales, hacía hincapié en la necesidad de tener debidamente en cuenta en el texto el hecho de que el derecho a la protección de los datos personales tiene el carácter de un derecho fundamental y que debe ser interpretado en las diversas disposiciones de la Directiva de modo que se garantice un alto nivel de protección, tal y como recuerdan los principios establecidos en la Recomendación R (87) 15 del Comité de Ministros del Consejo de Europa a los Estados miembros. En relación con el uso que las autoridades públicas pueden hacer legítimamente de los datos personales, el Grupo de Trabajo, sobre la base de la jurisprudencia del TJUE y del TEDH, insistía en la necesidad de garantizar que el

[1405] COMISIÓN EUROPEA - Comunicado de prensa (2015c), El acuerdo sobre la reforma de la protección de datos promovida por la Comisión reforzará el mercado único digital, Bruselas, 15 de diciembre de 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-6321_es.htm; Mark SCOTT (2015b), «Europe Approves Tough New Data Protection Rules», en *The New York Times*, Dec. 15. Disponible en Internet: http://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html?_r=1 [consulta: 27 de febrero de 2017].

[1406] ARTICLE 29 DATA PROTECTION WORKING PARTY (2015f), Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 3211/15/EN, WP 233, Adopted on 01 December 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf [consulta: 02 de marzo de 2017].

tratamiento se lleve a cabo de conformidad con las debidas garantías y salvaguardias por lo que refiere, por ejemplo, a la responsabilidad y la transparencia hacia los individuos. También se exigía mayor coherencia entre Directiva y Reglamento, en relación, por ejemplo, a las definiciones, a los principios, a las obligaciones y derechos y poderes de la persona, a la vista de la importancia cada vez más elevada de las interacciones entre el sector privado y la aplicación de la ley[1407]. En cuanto a aspectos específicos, la opinión consideraba de forma negativa la ampliación del ámbito de aplicación material de la Directiva destinada a cubrir también la prevención de riesgos para la seguridad pública, prefiriendo al respecto el texto original de la Comisión.

46. El 18 de diciembre de 2015 el Consejo (en particular, el Comité de Representantes Permanentes - COREPER) confirmó los textos transaccionales acordados con el Parlamento Europeo sobre la reforma de la protección de datos[1408] que se presentarían para su adopción por el Consejo, y posteriormente por el Parlamento, por lo que la previsión era ya en aquel momento que el Reglamento entrara en vigor en la primavera de 2018[1409].

2.5. La fase final: aprobación de la reforma por el Consejo de la UE y por el Parlamento Europeo

47. Por fin, el 8 de abril de 2016, el Consejo adoptó su posición en primera lectura[1410]. A continuación, el Parlamento Europeo adoptó el proyecto de Reglamento el 14 de abril de

[1407] En particular, el Grupo de Trabajo analiza una serie de aspectos (14) en los que formula, sugerencias, comentarios y observaciones, basándose en las directrices anteriores y sobre la jurisprudencia de los tribunales europeos sobre el tema: «*1/ Subject matter and objectives; 2/ Fairness of the processing; 3/ Purpose limitation; 4/ Data minimization; 5/ Distinction between the different categories of data subjects; 6/ Special categories of data; 7/ Processing of data relating to children; 8/ Profiling; 9/ Data subjects rights; 10/ Data controllers and processors' obligations; 11/ Transfers of personal data to third countries or international organizations; 12/ Role and powers of the supervisory authorities; 13/ Right to lodge a complaint; 14/ Previously concluded international agreements in the field of judicial co-operation in criminal matters and police co-operation*». También destaca la importancia de que la Directiva coloque el tratamiento correcto entre sus principios fundamentales. ARTICLE 29 DATA PROTECTION WORKING PARTY (2015f: 5 y ss.).

[1408] CONSEJO EUROPEO - Comunicado de prensa (2015), Reforma de la protección de datos en la UE: el Consejo confirma el acuerdo con el Parlamento Europeo, 951/15, 18.12.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/12/18-data-protection/ [consulta: 03 de marzo de 2017].

[1409] Roberto MAYOR GÓMEZ (2016), «Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)», en *GABILEX*, núm. 6, junio, pág. 8.

[1410] POSICIÓN DEL CONSEJO en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) - Adoptada por el Consejo el 8 de abril de 2016, 5419/1/16 REV 1, 2012/0011 (COD), Bruselas, 8 de abril de 2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_5419_2016_REV_1&qid=1463305162724&from=ES [consulta: 03 de marzo de 2017].

2016, completando así el *iter* legislativo. Al mismo tiempo, fue aprobada la Directiva (UE) 2016/680.

48. Este proceso[1411], tal como se anunció al comienzo de esta sección, se completó con la publicación el 4 de mayo de 2016 en el Diario Oficial de la UE de los textos de Reglamento europeo de protección de datos personales y de la Directiva que regula el tratamiento de datos personales en los ámbitos de la prevención, investigación y detección de los delitos. El RGPD (en inglés, *General Data Protection Regulation - GDPR*) entró en vigor 20 días después de su publicación, es decir el 24 de mayo de 2016. Desde ese tiempo transcurren los dos años para asegurarse de que los Estados miembros de la UE se conformen a las nuevas reglas – se aplica a partir del 25 de mayo de 2018[1412] – asegurando así la alineación perfecta (o casi) entre la legislación nacional[1413] y las disposiciones del RGPD que proporciona una

[1411] El estrecho diálogo institucional, no se limitó sólo al Parlamento Europeo, sino también a los órganos parlamentarios nacionales y las autoridades nacionales de protección de los datos, por un lado, y con el SEPD. Sobre la cooperación entre las instituciones, el SEPD publicó el 24 de mayo de 2016 el Informe Anual de 2015, que se centra en la adopción del nuevo sistema idóneo para garantizar una protección más eficaz, pero un amplio espacio está reservado, en particular, a la colaboración con el Grupo de Trabajo en el análisis de las consecuencias de la sentencia del TJCE en el caso *Schrems* y, por lo tanto, al tema de las soluciones para la transferencia transfronteriza de datos personales. SEPD (2016), Informe Anual 2015. Resumen ejecutivo, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 18. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/ar2015_summary_es.pdf [consulta: 03 de marzo de 2017].

[1412] Artículo 94 (Derogación de la Directiva 95/46/CE) del RGPD: «*1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018*»; también véanse artículo 99 (Entrada en vigor y aplicación) del RGPD: «*1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. 2. Será aplicable a partir del 25 de mayo de 2018*». Desde el punto de vista de José Luis Piñar Mañas esta norma europea hay que verla más como oportunidad que como amenaza: «*Hay que verlo como una oportunidad que permite esté en la agenda internacional la protección de datos. Tenemos que seguir hablando y mentalizándonos de la importancia de la protección de datos como derecho fundamental*». En Luisja SÁNCHEZ (2016), «José Luis Piñar: "Con el nuevo Reglamento Europeo de Protección de Datos se abre una puerta a la privacidad a nivel internacional que debemos aprovechar"», en *Law&Trends*, 02/05/2016. Disponible en Internet: http://www.lawandtrends.com/noticias/tic/con-el-nuevo-reglamento-europeo-de-proteccion-de.html [consulta: 04 de marzo de 2017].

[1413] La entrada en vigor de este nuevo Reglamento plantea la duda de cómo va a convivir en España con la LOPD. A este respecto, tanto José Luis Piñar Mañas como Pablo García-Mexia, apuntaban que la ley española seguiría siendo aplicable en lo que esté fuera del Derecho de la UE, pues, además, el Reglamento hace numerosas remisiones a la legislación nacional de los Estados miembros. También apuntaban a que la entrada en vigor del RGPD y su posterior aplicabilidad puede plantear problemas de convivencia con la legislación actualmente vigente, la LOPD. Igualmente, también cabe preguntarse sobre el papel de la AEPD y el valor que tendrán sus circulares en el nuevo contexto. *Cfr*. «El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales a la abogacía», en *Noticias Jurídicas*, 30/04/2016. Disponible en Internet: http://noticias.juridicas.com/actualidad/noticias/11047-el-nuevo-reglamento-europeo-de-proteccion-de-datos:-un-texto-complejo-que-abre-nuevas-perspectivas-profesionales-a-la-abogacia/ [consulta: 04 de marzo de 2017]. La misma prospectiva, la expone Alejandro Padín Vidal: «*Lo cierto es que, mientras la LOPD siga estando en vigor y no sea modificada, la norma nacional seguirá siendo de obligado cumplimiento y no podrá ser desterrada voluntariamente por ningún sujeto obligado. No obstante, ya advertimos que será necesario adoptar medidas de carácter legislativo en España a lo largo de los próximos dos años para evitar, a la finalización del referido plazo, los problemas de convivencia que se generarían entre la redacción actual de la LOPD y su norma de desarrollo, por un lado, y el RGPD, por otro lado*». En Alejandro PADÍN VIDAL (2016), «Nuevo Reglamento General de Protección de Datos de la Unión Europea», en *Lefebvre - El Derecho*, 22.04.2016. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/Reglamento-General-Proteccion-Datos-Union-Europea_11_943930002.html#a_comments [consulta: 04 de marzo de 2017].

disciplina uniforme y válida en términos de privacidad en toda Europa, con el fin de garantizar un nivel coherente y elevado de protección, y de remover los dificultades a la circulación de los datos personales en la Unión Europea[1414].

49. La Directiva, en cambio, entró en vigor el 5 de mayo de 2018, y desde ese momento obliga a los Estados miembros a transponer su contenido al derecho nacional en el plazo de 2 años[1415]. La nueva Directiva europea, sobre transmisión de datos para cuestiones judiciales y policiales, se aplica al intercambio de datos transfronterizos dentro de la UE y establecerá estándares mínimos para el tratamiento de datos en cada país. La intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales, sea como víctimas, acusados o testigos, mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. Se han incluido salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación transfronteriza más rápida y efectiva entre las autoridades policiales y judiciales, con el fin de combatir más eficazmente el crimen y el terrorismo en toda Europa.

50. Por último, la necesidad de coherencia entre los textos del RGPD y la Directiva policial está siempre presente en el texto de esta última; de hecho, se han hecho todos los esfuerzos para que las nociones, ideas, principios e incluso estructuras se dupliquen del Reglamento a la Directiva. Se debe prestar atención al hecho de que se trata de un proceso unidireccional, es decir, del Reglamento hacia la Directiva, como también se refleja en la atención mucho más limitada que recibió la Directiva durante su aprobación legislativa (en términos de reuniones reales celebradas en ella). Es innegable, como se evidencia también en los respectivos textos finales de los dos instrumentos, que las referencias se hacen en el texto de la Directiva al texto del Reglamento, pero no a la inversa. La supremacía no declarada del RGPD, que parece percibirse como anterior a la Directiva, puede resultar importante ya que las impugnaciones judiciales sobre el significado de los términos de la Directiva pueden surgir en el futuro[1416]. En el mismo contexto, es probable que los Estados

[1414] Nos encontramos con el único caso en el que un derecho fundamental recogido en Constitución Española (artículo 18, apartado 4) es regulado desde Europa, de aplicación directa, sin necesidad de transposición.
[1415] En el caso de Reino Unido e Irlanda, la Directiva sobre intercambio de datos para fines policiales y judiciales sólo se aplicará de manera limitada. Dinamarca podrá decidir en seis meses tras su adopción definitiva si quiere trasladar la directiva a la ley nacional. *Vid*. PARLAMENTO EUROPEO - Notas de prensa (2016b).
[1416] Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016: 10).

miembros apliquen el Reglamento de forma general, convirtiéndolo así en el texto de referencia también para la aplicación de la ley.

3. Dudas y aspectos críticos del RGPD, la necesidad de paradigmas comunes entre seguridad pública y derechos fundamentales

51. En un contexto histórico en el que se hace necesario fortalecer el sistema de protección de la privacidad de las personas, a la vez que se intensifican las actividades de seguridad nacional a través del intercambio de datos personales entre las autoridades competentes para combatir y prevenir casos terroristas, se hace especialmente necesario reducir la fragmentación jurídica existente con el fin de garantizar un nivel uniforme de protección de datos personales[1417]. En este propósito, el texto del RGPD[1418] es sin duda el pilar fundamental de la reforma del marco europeo, que se presenta como un sistema de reglas muy detallado y extenso (que consta de 11 Capítulos, 99 artículos y 173 considerandos previos[1419]), que proporciona una defensa más concreta contra la intrusión en la vida privada de los ciudadanos, incluidos los poderes públicos, y lo hace de manera uniforme considerando todas las facetas de los datos personales[1420].

[1417] David ERDOS (2015), «European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps» (September 1, 2015). A revised version of this paper is in the Journal of Law and Society (Winter 2016 Forthcoming); en *University of Cambridge Faculty of Law Research Paper*, núm. 30, págs. 31. Disponible en Internet: https://ssrn.com/abstract=2611583 or http://dx.doi.org/10.2139/ssrn.2611583 [consulta: 06 de marzo de 2017]. En esta contribución, el autor destaca la existencia de una brecha significativa dentro de los Estados europeos nacionales individuales en la protección de datos con referencia específica al uso de nuevas tecnologías.

[1418] Para un examen detallado del nuevo Reglamento, *cfr*. Franco PIZZETTI (2016b), *Privacy e il diritto europeo alla protezione dei dati personali: Il Regolamento europeo 2016/679*, Torino, G. Giappichelli Editore, págs. 208; José Luis PIÑAR MAÑAS (dir.) María ÁLVAREZ CANO, Miguel RECIO GAYO, (coords.) (2017), *Reglamento general de protección de datos hacia un nuevo modelos europeo de privacidad*, Madrid, Editorial Reus, págs. 851; José LÓPEZ CALVO (2017b), *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin - Servicio de Propiedad, págs. 329; José LÓPEZ CALVO (2018), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Madrid, Wolters Kluwer, págs. 850; Giovanni M. RICCIO, Guido SCORZA, Ernesto BELISARIO (a cura di) (2018), *GDPR e Normativa Privacy Commentario*, IPSOA; Christopher KUNER, Lee BYGRAVE and Christopher DOCKSEY (2019), «Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)», en *Commentary on the EU General Data Protection Regulation (GDPR)*, Forthcoming in 2019 from Oxford University Press, págs. 148; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[1419] El TJUE ha establecido claramente que el preámbulo de un acto legislativo europeo carece de fuerza jurídica vinculante y no puede invocarse para derogar las disposiciones del acto en cuestión. Sin embargo, los considerados introductorios a un acto legislativo de la Unión han sido utilizados por los tribunales europeos para interpretar disposiciones ambiguas del mismo acto. *Cfr*. Tadas KLIMAS and Jūratė VAIČIUKAITĖ (2008), «The Law of Recitals in European Community Legislation», en *ILSA Journal of International and Comparative Law*, vol. 15, págs. 16 y ss. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604 [consulta: 06 de marzo de 2017].

[1420] Algunos autores se han referido al RGPD como a un "código", para señalar la grandeza de la nueva normativa con respecto de la relativa pequeñez de la normativa anteriormente vigente (7 Capítulos, 34 artículos

52. Conforme a su artículo 1, su objeto – al igual que la Directiva de 1995 – es regular «*las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos*», así como la protección de «*los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*». También se contempla como principio programático que «*la libre circulación de los datos personales*» en la UE «*no podrá ser restringida ni prohibida*» por motivos concernientes con la protección de las personas físicas en relación con el tratamiento de datos personales[1421]. Por tanto, las personas físicas son los únicos beneficiarios de las normas de protección de datos y sólo los seres vivos están protegidos por la ley europea de protección de datos[1422]. El RGPD especifica con precisión los datos personales como cualquier información relacionada con una «*persona física identificada o identificable*»[1423].

53. Por lo tanto, el Reglamento pretende generar confianza y facilitar el control de los datos a sus titulares (ahora "interesados"), lo que no resulta tarea fácil. Esto lleva a un conflicto de intereses que deberán ponderarse para que el tratamiento de los datos personales cumpla con una de sus misiones: «*servir a la humanidad*». Para garantizar la efectividad del

---

y 72 considerandos de la Directiva de 1995): «*What we are likely to end up with is a data protection code with detailed provisions; EU data protection is in effect becoming a locus of regulation of very concrete things rather than a principle-driven human rights system*». En Paul DE HERT (2015), «The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?», en *Utrecht Journal of International and European Law*, vol. 31, núm. 80. Disponible en Internet: https://utrechtjournal.org/articles/10.5334/ujiel.cz/ [consulta: 06 de marzo de 2017]. Otros autores, como Franco Pizzetti, tienen dudas sobre la técnica jurídica utilizada por el legislador europeo, que en algunas partes del texto, dada la generalidad deseada, permite unas interpretaciones muy diferentes y, por otro lado, debido a la naturaleza rígida de ciertas normas parece tan limitada que la protección de datos incluso se debilita con respecto a la protección más flexible de la Directiva anterior. También, hay preocupaciones por el hecho de que, con respecto a las definiciones de los principios y conceptos de la materia, una vocación maniaca por los detalles puede introducir una rigidez excesiva y provocar un envejecimiento prematuro de esta norma. *Vid*. Franco PIZZETTI (2016b: 150). La misma observación la hacen Javier Puyol como Paula Ortiz, haciéndose la pregunta «*¿Un Reglamento nacido viejo?*». Los dos apuntaron un dato preocupante de cara al futuro: el Reglamento no contempla específicamente cuestiones como el "*Big Data*", el "*Cloud Computing*", la "Internet de las cosas" o "*BiTech*". Por tanto, puede pensarse que se ha perdido una ocasión para adaptar completamente la norma al entorno digital para permitirla envejecer bien. *Vid*. «El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales a la abogacía», en *Noticias Jurídicas*.

[1421] «*El artículo 1.1 consagra la privacidad de los datos por parte del ciudadano y la libre circulación de los datos*». Según José Luis Piñar esta segunda parte del enunciado es una de las cuestiones que más ha tenido que negociarse para la aprobación del texto final. Luisja SÁNCHEZ (2016).

[1422] Considerando 27 del RGPD.

[1423] Artículo 4 (Definiciones) del RGPD. Los beneficiarios de la protección otorgada por el Reglamento (UE) 2016/679 son sólo las personas físicas independientemente de su nacionalidad o lugar de residencia, con exclusión de las personas jurídicas. Sin embargo, los destinatarios de las obligaciones son los operadores económicos, sean micro, pequeñas y medianas empresas. *Vid*. considerando 14 del RGPD: «*La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto*».

derecho a la protección contra la intromisión en la vida privada, en sus nuevas formas, se ha identificado la herramienta flexible constituida por la interacción entre los derechos fundamentales: el RGPD proclama el derecho humano a la protección de datos personales como un derecho fundamental «*que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad*»[1424]. A continuación, señala el respeto a todos los demás derechos fundamentales reconocidos por las normas europeas y «*observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística*»[1425], en un equilibrio continuo regulado por el principio de proporcionalidad entre los instrumentos de investigación y la vida privada, tal y como exige la jurisprudencia del TJUE en los casos analizados anteriormente, en los que reafirmó el valor central de la *privacy*.

54. El *corpus* normativo constituye una importante voluntad de las instituciones europeas de introducir normas más rigurosas y estrictas, reduciendo así los márgenes de maniobra de los Estados en el tratamiento de los datos personales y la libre circulación de estos[1426]. De hecho, para limitar la injerencia en la vida privada por las distintas autoridades interesadas a nuestros datos personales, el RGPD reconoce el derecho a la protección de datos, a partir de la premisa indiscutible de que la protección de las personas físicas con respecto al tratamiento de los datos personales «*es un derecho fundamental*»[1427]: «*El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE)*

[1424] Considerando 4 del RGPD. *Vid*. Natalia MARTOS (2017), «Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo Reglamento de Protección de Datos?», en *Diario La Ley*, núm. 9081, Sección Tribuna, 15 de noviembre de 2017, Editorial Wolters Kluwer.
[1425] Considerando 4 del RGPD.
[1426] La mayor atención a los detalles y las especificaciones proporcionadas por el legislador europeo ha dado lugar a la creación de un marco reglamentario muy amplio, debido a la diversidad de propósitos a los que se refiere el nuevo RGPD. La Directiva de 1995 tuvo que configurarse como un instrumento ágil y delgado, que supliera la directriz para la armonización de las legislaciones nacionales, que luego sería llevado a cabo por los Estados miembros; mientras que el RGPD, al ser un acto normativo autoejecutable y obligatorio en todas sus partes, requiere una mayor exhaustividad y claridad de contenido, disciplinando en la manera más precisa posible los institutos de que se compone.
[1427] El texto del RGPD reitera algunos conceptos fundamentales que son la base de la misma Directiva 95/46/CE. El RGPD, actúa, en gran parte, como ya se contemplaba en la Directiva de 1995, manteniendo al mismo tiempo el concepto de privacidad basada en el consenso y el respeto de ciertos principios fundamentales (legalidad, proporcionalidad, equidad, transparencia, minimización de datos, *etc*.) y mantiene la dependencia de los reguladores nacionales a amplios márgenes de discrecionalidad.

establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan»[1428]. Como se puede comprobar el RGPD proclama el derecho a la protección de datos personales como un derecho fundamental de las personas de una manera más explícita que la Directiva anterior de 1995. En particular, este derecho se basa en el principio de la autodeterminación de la información, un concepto claramente expresado por el Tribunal Constitucional alemán en 1983[1429], que consideró este principio esencial para el desarrollo de la personalidad de un individuo. El Reglamento hace una reivindicación y reforzamiento del derecho humano a la privacidad y a la autodeterminación informativa. Se erige con firmeza como una potente declaración de principios, de reafirmación de las esencias de protección de datos en Europa, tanto en el espacio comunitario como frente al resto del mundo[1430], en especial China, Estados Unidos y Rusia.

55. No obstante, el RGPD hace referencia a la Carta de Niza, que afirmó la protección de datos como un derecho fundamental, independiente de la protección de la vida privada. A causa de la amenaza terrorista de los últimos años se han puesto en discusión certezas consolidadas. Y no sólo se habla, como hemos comentado, de revisar el Espacio Schengen, sino también de la considerable expansión de los poderes de la inteligencia con acceso sistemático a los datos personales de cualquier persona; de extensión del ámbito y la tipología de las interceptaciones; de atenuación, en resumen, de las garantías individuales por razones, precisamente, de la seguridad nacional[1431]. De hecho, entre sus objetivos

[1428] Considerando 1 del RGPD. En este sentido, han sido críticas las posiciones de *Access*, conocida organización internacional por los derechos digitales. Reconociendo que el texto es un paso adelante en comparación con la situación caótica actual, con veintiocho regulaciones diferentes, sin embargo, no resuelve todos los problemas. *Vid*. Raegan MACDONALD (2015), «As Privacy Regulation moves to trialogue, Access warns of dangerous loopholes in Council text», en *accessnow.org*, 15 June. Disponible en Internet: https://www.accessnow.org/as-privacy-regulation-moves-to-trialogue-access-warns-of-dangerous-loopholes-in-council-text/ [consulta: 08 de marzo de 2017].

[1429] BVerfG · Urteil vom 15. Dezember 1983 · Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil). Disponible en Internet: https://openjur.de/u/268440.html [consulta: 08 de marzo de 2017]. En particular, "autodeterminación informativa" significa el principio según el cual el individuo decide dentro de qué límites divulgar los hechos relacionados con su vida personal. Este derecho no es absoluto, sino que debe conciliarse con otros derechos y, en particular, con las necesidades de la sociedad para conocer los hechos relevantes para el público, además con la protección de los derechos de los demás y la prevención y represión de los delitos. Son derechos en conflicto, que, sin embargo, merecen protección y, por lo tanto, deben equilibrarse entre ellos. En este sentido, las necesidades de prevención y represión de los delitos también deben implementarse sin invadir formas inaceptables de vigilancia general de los ciudadanos. *Vid*. Pablo Lucas MURILLO DE LA CUEVA y José Luis PIÑAR MAÑAS (2009: 11-12).

[1430] José LÓPEZ CALVO (2018).

[1431] De hecho, la Corte di Cassazione (es decir el Tribunal Supremo italiano) declaró ilegítimas (con consiguiente inutilidad de los datos recogidos) las interceptaciones realizadas, de forma remota, a través de la introducción de virus informáticos en un teléfono inteligente (*smartphone*), ya que esto permite, más allá de los límites del decreto de autorización del juez de instrucción, captaciones en cualquier parte, en cualquier lugar y contexto en el que se encuentre el sospechoso, también activando la cámara del propio teléfono. Esta metodología, al permitir la captura de conversaciones sin limitaciones de lugar, contrasta, con el precepto constitucional establecido en el artículo 15 de la Constitución italiana. *Vid*. CORTE DI CASSAZIONE,

principales el Reglamento añade que «*Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica,* (…) *así como al bienestar de las personas físicas*»[1432], lo que garantiza un alto nivel de protección de datos en todos los sectores, incluida la cooperación judicial en materia penal y policial, para garantizar la correcta aplicación de las normas y definir normas eficaces de protección de datos a nivel global.

56. La necesidad de una protección de datos global es debida también al aumento significativo de la «*recogida y del intercambio*» de flujos transfronterizos de datos de carácter personal, que permite que la información personal intercambiada se utilice a gran escala «*sin precedentes*» entre los agentes públicos (y privados), planteando «*nuevos retos para la protección de los datos personales*»[1433]. Tal desarrollo, de acuerdo con el legislador europeo, requiere un marco «*más sólido*» y consistente para la protección de datos en la UE[1434], con el apoyo de medidas eficaces de aplicación, dada la importancia de crear el clima de confianza que permita el desarrollo de la «*economía digital* (…) *en el mercado interior*» (considerando 7). De acuerdo con lo establecido en este considerando, de hecho, las «*personas físicas deben tener el control de sus propios datos personales*» de modo que la confianza jurídica y práctica se vean reforzadas, tanto para los individuos como para los operadores económicos y las autoridades públicas, con el fin de «*facilitar aún más la libre circulación de datos personales en la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de datos personales*» (considerando 6).

57. Siempre relacionado con la función de «*mantener el equilibrio con otros derechos fundamentales* (…) *con arreglo al principio de proporcionalidad*», el considerando 10 del RGPD establece que el nivel de protección de los derechos y libertades de las personas físicas «*debe ser equivalente en todos los Estados miembros*». Es conveniente garantizar una aplicación «*coherente y homogénea*» de las normas sobre protección de los derechos y

Sezione VI, 26 maggio 2015-26 giugno 2015, n. 27100. Disponible en Internet: http://www.penale.it/page.asp?IDPag=1201 [consulta: 09 de marzo de 2017].

[1432] Considerando 2 del RGPD.

[1433] Considerando 6 del RGPD.

[1434] Natalia MARTOS (2017).

libertades fundamentales de las personas con respecto al tratamiento de datos personales en toda la Unión[1435]. «*En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal*», para realizar una misión de "interés público" o "inherente al ejercicio de los poderes públicos conferidos al responsable del tratamiento", los Estados miembros quedan libres «*para mantener o adoptar*» normas nacionales con el «*fin de especificar*» con mayor detalle la aplicación de las disposiciones del RGPD[1436]. Esto significa que los legisladores nacionales deberán adaptar los textos sobre todo para cubrir los vacíos que deja el Reglamento y aclarar las muchas dudas interpretativas que va a provocar el texto en su misión homogeneizadora.

58. De este modo, el RGPD no sólo innova la materia a través de la introducción de instituciones totalmente nuevas[1437], sino que lleva a cabo un trabajo para consolidar todas las posiciones y determinaciones de la jurisprudencia del TEDH y TJUE, del SEPD, del Grupo de Trabajo[1438] y autoridades nacionales, y, finalmente, confirma, amplía y actualiza el conjunto de principios derivados de la Directiva de 1995, dictando una disciplina más

[1435] El RGPD «*presuntamente se unifica*» y moderniza la normativa europea sobre protección de datos, permitiendo a los ciudadanos un mejor control de sus datos personales y a las empresas aprovechar al máximo las oportunidades de un mercado único digital, reduciendo la burocracia y beneficiándose de una mayor confianza de los consumidores. *Vid*. Ricard MARTÍNEZ (2016), «Desde un punto de vista jurídico la privacidad es un derecho cuya titularidad es irrenunciable», en *Lefebvre - El Derecho*, Madrid, 28.01.16. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/dia-europeo-proteccion-datos-privacidad-derecho-irrenunciable_14_912070001.html [consulta: 10 de marzo de 2017]. Respecto a las grandes novedades sobre el plan de la tutela de los derechos el mismo *Garante per la protezione dei dati personali* de Italia, Antonello Soro, declara que el Reglamento «*raggiunge l'ambizioso obiettivo di assicurare una disciplina uniforme ed armonizzata tra tutti gli Stati membri, eliminando definitivamente le numerose asimmetrie che si erano create nel tempo*». En «Pacchetto protezione dati in G.U.U.E.: Soro, giornata importante per i cittadini europei. Disciplina uniforme contro ogni barriera», en *Garante per la protezione dei dati personali*, Roma, 4 maggio 2016. Disponible en Internet: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4966337 [consulta: 10 de marzo de 2017].

[1436] Considerando 10 del RGPD: «(…) *Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito*».

[1437] Entre las grandes innovaciones, sólo por nombrar algunas que por el RGPD, se incluye la figura del Delegado de Protección de datos (DPO), el derecho al olvido, la ventanilla única, mayor protección de los datos de los menores de edad, y sanciones más altas.

[1438] El Grupo de Trabajo adoptó en la reunión plenaria de octubre de 2017, algunas medidas importantes, útiles para interpretar de manera correcta y uniforme en todos los países de la Unión Europea el Reglamento (UE) 2016/679. El Grupo ha dado el visto bueno definitivo a las Directrices sobre el *Data Protection Impact Assessment* (*DPIA*), la evaluación de impacto sobre la protección de datos que es responsabilidad del responsable del tratamiento cuando el tipo de tratamiento presenta riesgos elevados para los derechos y libertades de las personas. ARTICLE 29 WORKING PARTY - Press Release (2017), October 2017 Plenary Meeting. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [consulta: 11 de marzo de 2017].

oportuna, clara y, en la medida de lo posible, que satisfaga los requisitos de exhaustividad de los contenidos.

59. En este sentido, el nuevo texto afirma expresamente que «*para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia* (…) *y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales* (…)*, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*»[1439]. Estos propósitos no van a ser fáciles de aplicar en los 28 Estados miembros de la Unión Europea (mismos criterios, directrices, pautas para proteger los derechos, para sancionar cuando corresponda y para adoptar las mismas medidas ante los riesgos). Adicionalmente se permitirá, según lo que establece en el considerando 8, que las normas del Reglamento sean «*especificadas*» o «*restringidas*» por el Derecho de los Estados miembros, «*en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento*» (considerando 8). Asimismo, como ya se mencionó, los Estados miembros están facultados para «*adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación*» del RGPD (considerando 10).

60. Finalmente, en esta primera lectura del objeto del RGPD, debe tenerse en cuenta el alcance innovador del nuevo instrumento legislativo surgido para las necesidades de protección de datos personales dentro de una economía cada vez más caracterizada por el desarrollo tecnológico y telemático, de los innumerables intercambios de datos sensibles de las personas y en el poner una barrera, y con la que se espera luchar contra de la intromisión del Estado en nuestra vida privada con el objetivo de mejorar la seguridad pública. Para conseguir este desafío, las instituciones europeas, como acabamos de examinar en el texto legislativo, aseguran que el RGPD establecerá un único conjunto de normas sobre protección

[1439] Considerando 13 del RGPD.

de datos, válidas en toda Europa, ya que el marco jurídico basado en la Directiva 95/46/CE, no ha impedido la fragmentación de la aplicación de las normas sobre protección de datos personales en la Unión Europea[1440]. Pero ¿realmente el RGPD ha conseguido estandarizar la normativa europea proporcionando unas normas que garanticen una protección efectiva contra los Estados que utilicen datos personales en una "escala sin precedentes" frente a las amenazas contra la seguridad pública?

61. Después de esta primera parte introductoria en la que se han observado los motivos subyacentes del nuevo RGPD, procederemos a describir algunos de los cambios principales que introduce, tratando de enmarcarlos en el contexto de problemas relacionados con el tratamiento de datos de carácter personal por parte de los Estados, incluida la protección frente a las amenazas a la seguridad pública y los nuevos principios cardinales de protección de datos personales. En segundo lugar, se analizarán los límites reconocidos para la aplicación material del RGPD y otras limitaciones a la privacidad que los Estados puedan imponer. Por último, se analizarán los riesgos que, en el panorama actual, la transmisión y flujos de datos constantes a los que estamos inevitablemente sujetos se han multiplicado exponencialmente, al ser más accesibles y fáciles de procesar por las autoridades.

3.1. Los nuevos principios reconocidos por el RGPD, entre el derecho de los ciudadanos a la protección de sus datos y la garantía de la seguridad: ¿una combinación imposible?

62. Debe tenerse en cuenta de partida que el RGPD se diferencia de la Directiva 95/46/CE, ya que, mientras que esta última trató de proteger en primera instancia la libre circulación de datos[1441], dedicandose sólo secundariamente a la protección de los derechos individuales, mientras que el Reglamento revela una intención de actualizar la normativa otorgando una mayor protección a los derechos de las personas mediante la concesión de derechos específicos a los individuos y más obligaciones a las personas encargadas del tratamiento de datos personales. El RGPD, sobre la base del equilibrio de las libertades fundamentales, confirma y actualiza los principios y definiciones de referencia en lo que

[1440] En este sentido, en el noveno considerando del RGPD establece que los objetivos y principios de «*la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas* (…). *Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE*» (considerando 9). Esta exigencia, sin embargo, no agota su significado dentro de nuestras fronteras, pero es aún más importante en un momento en que la necesidad de armonización se encuentra ligada a las necesidades de carácter global, tales como la lucha y la prevención de amenazas a la seguridad colectiva.

[1441] *Vid*. artículo 1 de la DIRECTIVA 95/46/CE.

respecta al tratamiento de datos personales ya reconocidos anteriormente en la Directiva de 1995 sobre la protección de datos para garantizar el derecho a la protección de datos personales en el futuro.

63. La nueva normativa refuerza el principio de tratamiento vinculado a finalidades específicas[1442], introduciendo varios requisitos para considerar que el consentimiento es válido[1443]. Esta vinculación entre consentimiento y finalidades específicas figura en el artículo 5 (Principios relativos al tratamiento), cuando señala que los datos personales deben ser: *a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines* (…)*; c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales»* (…) *(«limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)*[1444]. En

[1442] El objetivo es sin duda facilitar las condiciones de legalidad del tratamiento, relativa a los derechos mediante la construcción de un sistema más claro, homogéneo, autónomo y coordinado, de manera que la lectura sea más fácil y ágil. El objetivo es también resaltar las innovaciones hechas en esta disciplina.

[1443] José LÓPEZ CALVO (2017a), «Las crecientes exigencias del consentimiento y el control institucional del clausulado en protección de datos», en *Diario La Ley Sección Ciberderecho*, Editorial Wolters Kluwer, núm. 10, 11 de septiembre.

[1444] El texto del RGPD se concentra principalmente en los procesos, actividades, medidas organizativas y técnicas, sanciones y obligaciones destinadas al responsable del tratamiento, mientras que la Directiva 95/46/CE en cambio se centraba exclusivamente en los derechos del interesado. Este es el punto de vista desde el que hay que leer el artículo 5 del RGPD. Los deberes y responsabilidades del responsable del tratamiento, como motor para la aplicación efectiva de los principios de protección de datos, fue señalada ya en una opinión del Grupo de Trabajo, en la que se sugirió la introducción de medidas y procedimientos para hacer efectivos los principios de protección de datos existentes, asegurando su eficacia y mientras se introduce el requisito de demostrar el cumplimiento si las autoridades de protección de los datos las solicitan. En esta opinión, el Grupo de Trabajo, anticipando conceptos que ahora se formalizan claramente en el RGPD, indicó una serie de medidas destinadas a seguir el principio de "*accountability*" («*responsabilidad proactiva*») entre los cuales se encuentra la aplicación de toda una serie de procedimientos y reglamentos internos para garantizar la eficacia de la gestión de los aspectos fundamentales relacionados con el tratamiento de datos personales. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2010b), Opinion 3/2010 on the principle of accountability, Adopted on

síntesis, el artículo 5 establece los principios que rigen el tratamiento de los datos personales. Estos principios cubren: "licitud, lealtad y transparencia"; "limitación de la finalidad"; "minimización de datos"; "exactitud de los datos"; "limitación de conservación"; "integridad y confidencialidad".

64. Los principios sirven "como punto de partida para disposiciones más detalladas en los artículos posteriores del Reglamento", y también toda legislación posterior de protección de datos debe cumplir con estos principios y deben tenerse en cuenta al interpretar dicha legislación. Con arreglo a la legislación de la UE, las restricciones a los principios de tratamiento sólo se permiten en la «*medida en que correspondan*» a «*los derechos y obligaciones*» previstos en los artículos 12 a 22 y deben respetar la esencia de los derechos y libertades fundamentales (artículo 23). Cualquier limitación a estos principios clave puede ser proporcionada a nivel de la UE o nacional; deben estar previstos por la ley, perseguir un objetivo legítimo y ser medidas necesarias y proporcionadas en una sociedad democrática. Las tres condiciones deben cumplirse.

3.1.1. Limitaciones a los principios clave de la normativa europea de protección de datos

65. Una de las novedades introducidas por el RGPD se centra en la aplicación del principio de transparencia que, según el artículo 5, apartado primero, letra a), es, quizás, el principio que ha sido objeto de una mayor intervención normativa por el legislador europeo, destinada a reforzar su alcance[1445], subrayando así que no se trata de una solución sencilla, rápida y eficaz para obtener una base suficiente que legitime el tratamiento. El "principio de transparencia" exige que «*toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro*» (considerando 39). Se hace referencia, en particular, a la información de las personas afectadas sobre la identidad del responsable del tratamiento y los fines del

13 July 2010, 00062/10/EN, WP 173, págs. 4. Disponible en Internet: europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf
[consulta: 14 de marzo de 2017].

[1445] Alejandro PADÍN VIDAL (2016). La Sección 1 (Transparencia y modalidades) del Capítulo III (Derechos del interesado) del RGPD está, de hecho, enteramente dedicada a este principio. Según José Luis Piñar Mañas, en cuanto a los derechos del interesado, con esta nueva norma se acabaron los conocidos en España como "derecho ARCO" (Acceso, Rectificación, Cancelación y Oposición). Supone, por tanto, una ampliación de los "derecho ARCO". «Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)», en *Noticias Jurídicas*, 04/05/2016. Disponible en Internet: http://noticias.juridicas.com/actualidad/noticias/11050-contenido-y-novedades-del-reglamento-general-de-proteccion-de-datos-de-la-ue-reglamento-ue-2016-679-de-27-de-abril-de-2016/ [consulta: 15 de marzo de 2017].

tratamiento y la información adicional para "garantizar un trato correcto y transparente «*con respecto a las personas físicas afectadas*» y sus derechos a obtener confirmación y comunicación de los datos del procesamiento de datos personales que les conciernan[1446]. Los datos personales «*deben ser adecuados*», relevantes y «*limitados*» en la medida necesaria para su tratamiento. De ahí la obligación, en particular, de garantizar que el período de retención de los datos personales se limite al mínimo necesario. "Los datos personales deben manejarse de forma que se garantice su seguridad y protección, incluso para evitar el acceso no autorizado o el uso no autorizado de los datos personales" (considerando 39).

66. El consentimiento en virtud del Reglamento se amplia y requiere una acción clara y afirmativa «*que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen*»[1447], de manera que el interesado debe poder conocer en todo momento quién, cómo y para qué están tratando sus datos personales, así como qué datos personales exactamente están siendo tratados e incidencias que se produzcan sobre los mismos. Por lo tanto, según el artículo 4, apartado 11, se exige que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco, excluyéndose la posibilidad de un consentimiento tácito o pasivo[1448] *expressis verbis*. Para poder considerar que el

[1446] Considerando 39 del RGPD. Las personas físicas deben ser alertados sobre los riesgos, las reglas, las garantías y los derechos relacionados con el tratamiento de los datos personales y la forma en que se ejercen sus derechos. En particular, los "fines específicos del procesamiento" de los datos personales deben "ser explícitos, legítimos y precisos" cuando se recopilan datos personales. «*Los datos personales sólo deben*» procesarse si el propósito del procesamiento no es «*razonablemente*» posible «*por otros medios*». Para garantizar que los datos personales "no se guarden durante más tiempo del necesario", «*el responsable del tratamiento*» debe establecer un plazo para la cancelación o la verificación periódica. Deben «*tomarse todas las medidas razonables*» para asegurar que los datos personales inexactos sean rectificados o eliminados.

[1447] *Amplius*, *vid*. considerando 32 y artículo 7 (Condiciones para el consentimiento) del RGPD. Es explícito también en el sentido de que se exige un «*lenguaje claro y sencillo*». *Vid*. considerando 42. Efrén DÍAZ DÍAZ (2017), «La nueva LOPD: un paso para la adaptación legal a la nueva realidad social y digital», en *Lefebvre - El Derecho*, 23.11.2017. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/LOPD-adaptacion-realidad-social-digital_11_1161430002.html [consulta: 15 de marzo de 2017]. En conformidad con el RGPD, la nueva LOPD quiere asegurar que el consentimiento de las personas para el tratamiento de sus datos proceda de una declaración o de una acción clara y afirmativa.

[1448] El legislador a nivel semántico, de hecho, es claro y meridiano y, si en la definición derivada de la Directiva del 1995, artículo 2, se presentó el consentimiento como «*toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan*», el nuevo apartado 11 del artículo 4 (Definiciones) del RGPD especifica la definición del «*consentimiento del interesado*»: «*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*». Adicionalmente, se prevé la obligación de que el consentimiento del afectado para una pluralidad de finalidades de procesamiento de datos conste que se otorga de manera específica e inequívoca para cada una de ellas. Ya no cabe obtener ni prestar un consentimiento genérico o difuso para múltiples finalidades. Miguel RECIO GAYO (2017c), «El consentimiento en el RGPD: comentarios al borrador de Directrices del Grupo de trabajo del artículo 29», en *Diario La Ley*, Sección Ciberderecho, núm. 1, 19 de diciembre.

consentimiento es "inequívoco", se requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado, de manera que el consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos. La nueva regulación excluye el consentimiento tácito, derivado de la manifestación de la negativa del afectado al tratamiento de sus datos, normalmente obtenido por la vía de no responder a una comunicación previa de la empresa o entidad responsable del tratamiento.

67. Asimismo, para preservar la libertad de expresión de la voluntad del interesado, el considerando 43 excluye que «*el consentimiento*» pueda constituir «*una base jurídica válida para el tratamiento*» en situaciones en las que existe un claro desequilibrio entre el interesado y el responsable del tratamiento, especialmente cuando el responsable del tratamiento es «*una autoridad pública*», lo que pone en cuestión que el consentimiento se exprese libremente en ese tipo de situaciones[1449]. Se supone que el consentimiento no se ha expresado libremente si no es posible expresar un consentimiento por separado para el tratamiento de distintas operaciones de los datos personales, aunque apropiado en el caso propio, o si la «*ejecución de un contrato, incluida la prestación de un servicio*», es subordinada al consentimiento, aunque no necesario para tal ejecución (artículo 7, apartado 4).

68. Con respecto al principio de licitud del tratamiento (artículo 6), es lícito si el interesado "ha dado su consentimiento" para el tratamiento; si «*es necesario para la ejecución de un contrato*»; si «*es necesario para el cumplimiento de una obligación legal aplicable al responsable*»; si «*es necesario para proteger intereses vitales del interesado o de otra persona física*»; si «*es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*»; «*para la satisfacción de un interés legítimo perseguidos por el responsable del tratamiento o por un tercero*», siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales[1450]. Se autoriza a los Estados miembros, en virtud del artículo

[1449] Así lo críticaba el Grupo de Trabajo, según el cual el fundamento jurídico más apropiado, en caso de que el responsable del tratamiento de datos sea una entidad pública, debe encontrarse en las bases jurídicas que se rigen actualmente por el artículo 6, apartado 1, letras c) y e) (*vid*. *infra*). ARTICLE 29 DATA PROTECTION WORKING PARTY (2011b), Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, 01197/11/EN, WP187. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf [consulta: 16 de marzo de 2017].

[1450] Existe interés legítimo por parte del responsable cuando el titular de los datos puede tener «*las expectativas razonables de los interesados basadas en su relación con el responsable*». Considerando 47 del RGPD.

6, apartado 2, a especificar con mayor detalle esta enumeración, para lo que «*podrán mantener o introducir disposiciones más específicas*» a fin de adaptar su aplicación.

69. Al igual que el principio de proporcionalidad, el nuevo RGPD presenta una idea muy innovadora para su aplicación a la legislación nacional. El artículo 6, apartado 3, última frase establece que «*El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido*». Esta disposición, insertada en el marco de las condiciones de «*licitud del tratamiento*», representa la expresión del principio de proporcionalidad transpuesta al legislador estatal[1451], similar de alguna manera a lo que dispuso el TJUE en el caso *Tele2 Sverige*, sentencia posterior a la aprobación final y la entrada en vigor de la nueva normativa europea, y sin duda de acuerdo con la cláusula de proporcionalidad del artículo 52 de la CDFUE.

70. El tratamiento de datos personales «*con fines distintos de aquellos para los que hayan sido recogidos inicialmente sólo debe permitirse*» si es compatible con los fines para los que se recopilaron inicialmente los datos personales. En esta situación, no se pide ninguna base legal distinta de la que ha permiso la recopilación de datos personales. Si «*el tratamiento es necesario*» para la realización de una tarea de «*interés público*» o para «*el ejercicio de poderes públicos conferidos al responsable del tratamiento*», la legislación de la Unión o de los Estados miembros pueden establecer y especificar los fines y cometidos para los cuales «*se debe considerar compatible y lícito el tratamiento ulterior*». El tratamiento ulterior con fines de almacenamiento de «*interés público, investigación científica*» o «*histórica*» o con «*fines estadísticos*» debe considerarse un tratamiento legítimo y compatible. El fundamento jurídico establecido por «*el Derecho de la Unión o los Estados miembros para el tratamiento de datos personales*» también puede constituir una «*base jurídica para el tratamiento ulterior*»[1452]. A fin de establecer si la finalidad del tratamiento ulterior «*es compatible*» con la finalidad para la que se recopilaron inicialmente los datos personales, el responsable del tratamiento debe, después de cumplir «*todos los requisitos*» para la legalidad «*del tratamiento original*», tener en cuenta: «*a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a*

[1451] Los «*Estados miembros consultarán a la autoridad de control*» de protección de datos nacional durante la elaboración de propuesta de acto legislativo que será adoptada por los parlamentos nacionales o de medida reglamentaria basada en ese acto legislativo relativo al tratamiento. Artículo 36 (Consulta previa), apartado 4, del RGPD.
[1452] Considerando 50 del RGPD.

la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales (…)*; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización*»[1453].

71. Entre los nuevos principios innovadores, el RGPD introduce el concepto según el cual ya no es necesario "defender" a la persona del procesamiento de los datos que le conciernen, sino que la protección se puede integrar en el tratamiento mismo. Para que esto sea posible, es necesario intervenir en los datos, privándolos de algunos componentes de identificación mediante el uso de técnicas de «*seudonimización*», definida por el artículo 4, núm. 5, como el tratamiento de los datos personales, de modo que ya «*no puedan atribuirse*» a una persona en particular (interesado) sin el uso de «*información adicional, siempre que dicha información adicional*» se mantenga por separado y protegida por «*medidas técnicas y organizativas*» destinadas a evitar la identificación de personas físicas[1454]. Por tanto, podría decirse que la seudonimización consiste en un procedimiento alternativo para la reutilización de los datos que, de acuerdo con el principio de finalidad, ya no se corresponden con los requisitos por los que fueron recopilados y procesados y, como tales, deben eliminarse. De hecho, el principio general es que los datos deben ser conservados de una manera que permita la identificación de las personas interesadas "por un período de tiempo no superior a lo necesario para la consecución de los fines para los que fueron recogidos" o de otra manera suprimidos. El uso posterior de tales datos puede permitirse para otros fines, siempre que los datos mencionados anteriormente sean anonimizados o seudonimizados. Si la anonimización consiste en el procedimiento que permite el uso sólo después de que todos los elementos identificadores han sido eliminados[1455], la seudonimización es el proceso dirigido a

[1453] Artículo 6, apartado 4, del RGPD.

[1454] Por lo tanto, la «*introducción explícita*» de la «*seudonimización*» en el RGPD «*no pretende excluir ninguna otra medida relativa a la protección de los datos*», sino quetiene por objeto evitar que su aplicación eluda el sistema de protección descrito en la legislación europea. El considerando 28 del RGPD establece que la seudonimización a los datos personales «*puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos*».

[1455] *Vid*. considerando 26 del RGPD. Sin embargo, debe tenerse en cuenta que los datos anónimos ya no se consideran datos de carácter personal y, como tal, no están sujetos a las regulaciones que rigen la protección de los datos personales, mientras que los datos seudonimizados se consideran información sobre personas identificables indirectamente y por lo tanto sometidos a régimen regulador del RGPD. La decisión del legislador europeo de no establecer una definición de datos anónimos plantea dudas. Hubiera sido oportuno aprovechar esta oportunidad para establecer expresamente que la anonimización de los datos debe ser irreversible a fin de excluir la aplicación de la legislación de protección de datos personales. Se ha advertido la posibilidad de que incluso los datos aparentemente anónimos puedan rastrearse hasta el interesado, combinándolo con otra información, incluso anónima, gracias a las técnicas de "minería de datos" ("*Data Mining*"). Estas técnicas presentan un potencial considerable para la agregación de datos y la reelaboración de

"disimular" algunos identificadores que conducen de regreso a la identidad del sujeto sin eliminarlos del todo. Es fundamental que los datos así transformados no mantengan elementos de identificación que puedan conducir a la identidad de la persona anónima o seudonimizada.

72. Si la persona ha dado su consentimiento[1456] o «*el tratamiento se basa en el Derecho de la Unión o de los Estados miembros*» y «*constituye una medida necesaria y proporcionada en una sociedad democrática para proteger, en particular, los objetivos importantes de interés público general*»[1457], el responsable del tratamiento «*debe estar facultado para el tratamiento ulterior de los datos personales*», independientemente de la compatibilidad de los propósitos. En cualquier caso, debe garantizarse «*la aplicación de los principios establecidos*» en el RGPD[1458], en particular la obligación de informar a la persona interesada «*sobre esos otros fines y sobre sus derechos*», como también «*el derecho de oposición*». La indicación por parte del responsable de posibles delitos o «*amenazas a la seguridad pública*» y la transmisión de datos personales relevantes a una autoridad competente en «*casos individuales*» o en varios «*casos relacionados*» con el mismo delito o «*amenaza a la seguridad pública es interés legítimo*» perseguido por el responsable. Sin embargo, dicha divulgación en interés legítimo del responsable del tratamiento o el tratamiento posterior de datos personales debería prohibirse «*si el tratamiento no es*

los mismos con el fin de obtener perfiles individualizados muy precisos. En este sentido, *vid*. Mario VIOLA DE AZEVEDO CUNHA, Danilo DONEDA, Norberto Nuno GOMES DE ANDRADE (2010), «The Re-Identification of Anonymous Data and the Processing of Personal Data for Further Purposes: Challenges to Privacy (La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy) (in Italian)», en *Ciberspazio e Diritto*, vol. 11, núm. 4, págs. 641-655. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740383 [consulta: 18 de marzo de 2017].

[1456] Un elemento esencial para modular el alcance del consentimiento será la interpretación de la «*expectativa razonable del interesado*». Elemento de una cierta volatilidad previsiblemente mudable con el tiempo. La "expectativa" se vincula a un momento y contexto pudiendo, por ello, variar de manera sobrevenida. El Reglamento recoge la necesidad de evaluar la "expectativa" vinculado al "consentimiento". José LÓPEZ CALVO (2017a).

[1457] Estos objetivos son, entre otros, «*la seguridad del Estado*»; «*la defensa*»; «*la seguridad pública*»; «*la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención*». Otros objetivos importantes de interés público general de la Unión o de un Estado miembro que se incluyen son: «*el interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario*»; «*la sanidad pública y la seguridad social*»; «*la protección de la independencia judicial y de los procedimientos judiciales*»; «*la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas*»; «*una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública*»; «*la protección del interesado o de los derechos y libertades de otros*»; «*la ejecución de demandas civiles*». Artículo 23 del RGPD.

[1458] Considerando 50 del RGPD. Obligaciones y derechos «*establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22*».

compatible con una obligación» jurídicamente vinculante de carácter profesional, legal, profesional o de otro tipo[1459].

73. Así los poderes públicos quedan emplazados para modular en un delicado y complejo ejercicio de ponderación entre interés público/seguridad y privacidad y en concreto para especificar en cada momento y situación en cada relación. El RGPD plantea la necesidad de localizar de partida cuál será la base legitimadora del tratamiento, que incluye otras cinco además del consentimiento[1460]. El consentimiento no es siempre necesario, pero cuando se exija tiene que ser real[1461]. Es previsible en este (y otros) aspectos una implicación creciente de control de las autoridades, como se ha explicado en esta investigación, en los que no concurre el consentimiento como base.

74. Es indudable, de hecho, como los principios examinados están estrechamente relacionados en profundidad con los derechos de los interesados como de la transparencia y modalidades de la información, de las comunicaciones al interesado, ya que la transparencia está vinculada al funcionamiento de los derechos principalmente el derecho de acceso[1462]. Por lo tanto, a continuación, el Capítulo III del RGPD (artículos 12 a 22) se refiere a estos "derechos de los interesados", que suponen la introducción de nuevos derechos en el ámbito de la protección de datos. El artículo 12 a este respecto establece una obligación real para que «*el responsable del tratamiento*» adopte todas «*las medidas apropiadas*» para proporcionar a los interesados la información a que se refieren los artículos 13 y 14 (información que deberá facilitarse cuando los datos personales se obtengan del interesado, o información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado), o las comunicaciones a las que se hace referencia en los artículos 15 a 22 (es

[1459] Considerando 50 del RGPD.

[1460] Artículo 6, apartado 1, del RGPD: «*El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño*».

[1461] José LÓPEZ CALVO (2017a).

[1462] Se puede resumir en un esquema con una estructura triangular en cuyos vértices encontramos respectivamente transparencia, información y ejercicio de los derechos. Es decir, sin transparencia no hay información (o al menos es difícil obtener una imagen completa, clara y veraz), si no hay información no puede seguir un ejercicio eficiente de los derechos por parte de los interesados. Para cerrar el esquema y completarlo, los tres elementos son necesarios, de hecho, siendo en efecto el uno el presupuesto del otro.

decir, el conjunto completo de derechos y obligaciones que comienzan por el derecho de acceso y terminan con la disposición relativa al proceso automatizado de toma de decisiones con respecto a las personas físicas, incluidos los perfiles) y el artículo 34 (que prevé las comunicaciones en caso de violación de los datos personales de la parte interesada). Es esencial que dicha información y comunicaciones se desarrollen «*en forma concisa, transparente, inteligible y de fácil acceso*», con un lenguaje simple y claro[1463], acerca de los fines, modalidades, alcance del tratamiento y la identidad y los datos de contacto del responsable y deben ser capaces de ejercer sus derechos sobre sus datos con más facilidad que en la actualidad con el fin de expresar el "consentimiento informado y claro"[1464].

75. La transparencia de los datos y la forma en que se lleva a cabo el tratamiento debe servir, por lo tanto, para que el interesado siga sus datos, autorice cambios, solicite actualizaciones y prohíba y solicite intervención para evitar abusos. Con el fin de mejorar la protección, se prevén obligaciones adicionales para el «*responsable del tratamiento*», que «*facilitará al interesado el ejercicio de sus derechos*» y que no puede negarse a satisfacer la solicitud de la parte interesada para ejercer estos derechos, estando obligado a proporcionar información al interesado relativa «*a sus actuaciones sobre la base de una solicitud*» en un plazo máximo de un mes, prorrogable por dos meses[1465]. Así, el principio de transparencia parece exclusivamente *ex post*, es decir, en una etapa posterior del tratamiento, que en este caso ya se asumió, como un requisito que debe cumplirse para que el complejo de comunicaciones e información solicitado por el interesado cumpla con respecto al dictado normativo que requiere la máxima comprensión y la "clara" posibilidad de conocer por parte de las personas a quienes pertenecen los datos. De hecho, el principio de transparencia ya debe estar presente en un momento anterior al conjunto de operaciones al que se someterán posteriormente los datos, es decir, incluso antes de que el responsable de datos llegue a poseer los datos del usuario, en una fase en la que la transparencia y el consentimiento del interesado están estrechamente relacionados. La persona a la que pertenecen los datos debe poder prefigurar antes de un consentimiento válido cuál será el uso de los datos, a qué operaciones de trato serán sometidos los mismos, por cuánto tiempo, con qué modalidades

[1463] Artículo 12 (Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado) del RGPD.
[1464] En particular: artículo 13 (Información que deberá facilitarse cuando los datos personales se obtengan del interesado); y artículo 14 (Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado).
[1465] Artículo 12, apartados 2 y 3, del RGPD.

y cuáles son los fines específicos para los que se procesan. Sólo así se puede decir que el interesado está realmente y completamente informado sobre la transferencia y el uso de sus datos personales a los que ha dado su consentimiento. De esta manera puede considerarse que se respeta "el derecho a la autodeterminación que es la sustancia del derecho a la protección de los datos personales".

76. Además, el principio de transparencia está firmemente vinculado al derecho de acceso del interesado (artículo 15), que tiene una importancia estratégica significativa en la dinámica de los procedimientos, ya que es funcional, también podríamos decir prodrómica con respecto al ejercicio de otros tipos de derechos relacionados tales como rectificación (artículo 16), supresión o «*derecho al olvido*» (artículo 17), limitación del tratamiento (artículo 18)[1466], rectificación o supresión de datos personales o la limitación del tratamiento (artículo 19), portabilidad de los datos (artículo 20) y oposición (artículo 21).

77. Por lo tanto, la transparencia y el derecho de acceso adquieren una importancia significativa en la nueva normativa: la transparencia como regla metodológica a implementarse *ex ante* al tratamiento (como una de las condiciones de validez del consentimiento) y *ex post* al tratamiento (comunicaciones e información con respecto a operaciones realizadas en datos)[1467]; y derecho de acceso como una verificación realizada por el interesado para probar el cumplimiento de los principios subyacentes a un procesamiento correcto de sus datos y para tener, además, datos personales completos en un momento específico. Por lo tanto, cada interesado debe tener derecho a conocer y obtener comunicaciones, en particular en relación con la finalidad para los que se procesan los datos personales, cuando sea posible, el plazo de tratamiento de los datos personales, la existencia del derecho del interesado a pedir al responsable del tratamiento que rectifique o suprime los datos personales o limite el tratamiento de los datos personales que le conciernen o se oponga a su procesamiento y la lógica a la que se aplica cualquier tratamiento automatizado y, al menos cuando se basa en la elaboración de perfil, a las posibles consecuencias de dicho

[1466] *Vid. infra*.

[1467] El Grupo de Trabajo especifica que el cumplimiento con el artículo 12 (principio de transparencia) del RGPD debe garantizarse durante todo el ciclo de vida del tratamiento: antes de que comience, durante todo el período de su desarrollo, y siempre que ocurran hechos nuevos mientras el procesamiento está en progreso. *Amplius*, ARTICLE 29 DATA PROTECTION WORKING PARTY (2017c), Guidelines on transparency under Regulation 2016/679, 17/EN, WP260; Franco PIZZETTI (2017), «GDPR, cosa cambia con le nuove linee guida su trasparenza e responsabilizzazione», en *AgendaDigitale.eu*, 15 Dic 2017. Disponible en Internet: https://www.agendadigitale.eu/sicurezza/gdpr-cosa-cambia-con-le-nuove-linee-guida-su-trasparenza-e-responsabilizzazione/ [consulta: 21 de diciembre de 2017].

tratamiento[1468]. Conjuntamente, el apartado 2 del artículo 15 prevé que «*cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia*»[1469].

78. Continuando con la enumeración de los nuevos derechos de los ciudadanos, para identificar el alcance del RGPD en el objeto de nuestra investigación, entre los aspectos más innovadores que protegen a los individuos se encuentran los acuerdos destinados a reconocer el «*derecho a la portabilidad*» o el derecho a trasladar los datos a otro proveedor de servicios. Dado que "el derecho a la portabilidad de datos permite la transmisión directa de datos personales" de un responsable de tratamiento de datos a otro, se constituye en una herramienta importante para favorecer el libre flujo de datos personales en la UE. Este nuevo derecho implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable en determinadas condiciones[1470]. La finalidad de este nuevo derecho es empoderar al titular de los datos y otorgarle un mayor control sobre los datos personales que le conciernen.

[1468] En particular, según el artículo 15 (Derecho de acceso del interesado), apartado 1, del RGPD la información que se deben proporcionar son: «*a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado*».

[1469] Sobre las transferencias datos personales a un tercer país o a una organización internacional, véanse *infra*.

[1470] Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado. Artículo 20 (Derecho a la portabilidad de los datos) del RGPD: «*1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible*». El artículo 20 ha creado un nuevo derecho a la portabilidad de los datos, muy relacionado con el derecho de acceso a los propios datos regulado en el artículo 15 del RGPD, pero diferente del mismo en varios aspectos. Este derecho permite a los interesados «*recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento*». La finalidad de este nuevo derecho es empoderar al titular de los datos y darle más control sobre los datos personales que le conciernen. Carlos FERNÁNDEZ HERNÁNDEZ (2016), «Las autoridades europeas publican nuevas directrices para la aplicación del Reglamento Europeo de Protección de datos», en *Diario La Ley*, 19-12-2016.

79. En este punto se hace necesaria alguna explicación adicional sobre la portabilidad de los datos. El considerando 68 del RGPD, precisa que el derecho a la portabilidad de los datos «*debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato*», mientras «*no debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato* (…)*, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable*»[1471]. A partir de esto, está claro que este derecho no se puede ejecer frente a los responsables de datos que ejercen funciones públicas. Además, el ejercicio de este derecho a la portabilidad no puede afectar «*negativamente a los derechos y libertades*» de los demás[1472].

80. Los principios y derechos del interesado establecidos en el RGPD, sin embargo, pueden verse afectados por una cláusula de restricciones que recuerda el apartado 2 del artículo 8 del CEDH, al prever en el artículo 23 (Limitaciones) que la legislación de la Unión o de los Estados miembros «*podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos*» contemplados en el RGPD[1473] cuando «*tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro* (…)»[1474]. Por

[1471] *Cfr*. artículo 20, apartado 3, del RGPD. Los borradores iniciales generaron dudas sobre la posibilidad de que el interesado disfrute del derecho a la portabilidad de los datos, si el tratamiento se basa en otras condiciones de legitimidad. *Vid*. EDPS (2012: 25).

[1472] Artículo 20, apartado 4, del RGPD. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2017b), Guidelines on the right to data portability, adopted on 13 December 2016 As last Revised and adopted on 5 April 2017, 16/EN WP, 242 rev.01. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [consulta: 07 de abril de 2017].

[1473] Capítulo III (Derechos del interesado), Sección 5 (Limitaciones). Artículo 23, apartado 1, del RGPD: «*El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22* (…)».

[1474] Artículo 23, apartado 2, del RGPD: «*En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a: a) la finalidad del tratamiento o*

lo tanto, en relación con la aplicación de los principios del Reglamento[1475], se pueden imponer restricciones, en concreto: «*a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento*». Y todo ello, en la medida en que sea «*necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general* (…)»[1476].

81. En particular, el artículo 23 prevé toda una serie de casos en los que el Derecho de la Unión o de los Estados miembros puede imponer limitaciones específicas a los derechos de protección de datos garantizados por la normativa. Entre los fines que pueden justificar las restricciones figuran específicamente la "seguridad nacional", "la defensa", "la seguridad pública", "la prevención", "investigación", "detección o enjuiciamiento de infracciones

de las categorías de tratamiento; b) las categorías de datos personales de que se trate; c) el alcance de las limitaciones establecidas; d) las garantías para evitar accesos o transferencias ilícitos o abusivos; e) la determinación del responsable o de categorías de responsables; f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento; g) los riesgos para los derechos y libertades de los interesados, y h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta».

[1475] El RGPD contiene muchos principios fundamentales interesantes para proteger a las personas. Entre estos principios, interesante el contenido en el artículo 22 (Decisiones individuales automatizadas, incluida la elaboración de perfiles), apartado 1, que establece claramente que: «*Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*». El motivo de ese artículo lo encontramos en el considerando 71 del Reglamento: «*El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar* (…). *Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado* (…)».

[1476] Considerando 73 del RGPD

penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención"[1477].

82. En comparación con el marco regulatorio anterior, el nuevo RGPD también contiene especificaciones importantes sobre el contenido de las restricciones y los límites imponibles. En primer lugar, queda claro que la restricción debe ser «*necesaria y proporcionada en una sociedad democrática*» (artículo 23). Lo que evidentemente recuerda la fórmula contenida tanto en el CEDH como en la CDFUE. En segundo lugar, se prevé que la restricción, adoptada legislativamente, contenga algunas disposiciones específicas relativas a: a) las finalidades del tratamiento o de las categorías de tratamiento; b) las categorías de datos personales; c) el alcance de las limitaciones introducidas; d) garantías para evitar abusos o acceso o transferencia ilegal; e) la indicación precisa del responsable de datos; f) los plazos de retención y las garantias aplicables teniendo en cuenta la naturaleza, alcance y objetivos de las categorías de tratamiento o tratamiento; g) riesgos a los derechos y libertades de los involucrados; y h) el derecho de los interesados a ser informados de la limitación, a menos que ésto pueda poner en peligro los fines. Como se puede imaginar de las normas antes mencionadas, se espera que el test de legitimidad sobre futuras restricciones sea muy severo, "en línea con la jurisprudencia más reciente" del TEDH y del TJUE que son una referencia ineludible para resaltar los límites dentro de los cuales las restricciones a la protección de los datos personales se considerarán legítimas[1478].

83. Sin embargo, las excepciones podrían causar un efecto contrario al espíritu propio del RGPD, por lo que en su considerando 10 se afirma que «*debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea*». Si bien es cierto que ese mismo considerando reconoce cierto margen de maniobra a los Estados miembros[1479], introduce dicho margen «*a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento*»,

[1477] Del mismo modo *cfr*. la Directiva (UE) 2016/680 en su considerando 14 (*vid*. *infra*).
[1478] *Vid*. la jurisprudencia de ambos Tribunales *supra*.
[1479] Haciendo amplio uso de las facultades que atribuye a los Estados el RGPD, Alemania ha sido el primer país de la Unión Europea en aprobar una Ley de protección de datos adaptada al RGPD. El pasado 27 de abril de 2017 el Parlamento alemán aprobó la *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* o *Bundesdatenschutzgesetz-BDSG* (Ley Federal de Protección de Datos), norma que sustituirá a la actual normativa una vez que comience a ser aplicable el RGPD en mayo de 2018. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU). Disponible en Internet: https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2017/0301-0400/0332-17.html [consulta: 24 de mayo de 2017].

y no de restringir los derechos incluidos en el mismo al arbitrio de los Estados miembros, y en base a los ambiguos criterios del considerando 73. Esto significa que las leyes nacionales siguen siendo una parte importante del nuevo régimen de protección de datos, pues están llamadas a tener un efecto significativo en la aplicación del Reglamento y en la creación de un mercado único genuinamente armonizado. Por lo tanto, el desafío será cómo conjugar el principio de supremacía del Derecho europeo con la posibilidad de restringir determinados aspectos del RGPD por parte de los Estados miembros, en la manera revista de manera tan confusa en el artículo 23 en relación con el considerando 73.

84. A la luz de las consideraciones planteadas, ¿es suficiente que se plantee una vaga necesidad para salvaguardar seguridad del Estado, la seguridad pública u otros objetivos importantes de interés público general para eludir los principios de privacidad establecidos en el Reglamento? Parece que sí. Por lo tanto, los Estados, en defensa de la seguridad de los ciudadanos, pueden imponer limitaciones a los derechos de los interesados que repercutan en su propia privacidad, como se reflejan en el artículo 23 del Reglamento[1480].

3.1.2. El responsable del tratamiento y los riesgos de violación de los derechos y libertades fundamentales

85. El aumento de las obligaciones de los responsables del tratamiento de datos personales encuentra su razón de ser en la voluntad de evitar que los derechos otorgados a las personas puedan ponerse en peligro por una conducta ilícita. Los riesgos para los derechos y libertades de las personas pueden resultar del tratamiento de datos personales que puedan causar daños y perjuicios especialmente si el tratamiento puede llevar, por ejemplo, a los interesados a verse privados de sus derechos y libertades o impedidos para «*ejercer el control sobre sus datos personales*», en particular, en los casos en los que se evalúen

[1480] Lo dispuesto en el artículo 23 parece la copia del artículo 13 (Excepciones y limitaciones) de la anterior Directiva 95/46/CE: «*Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos* (…) *cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras* personas*. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados* (…) *cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas*».

aspectos personales, preferencias o intereses personales, comportamientos, situaciones o «*movimientos, con el fin de crear o utilizar perfiles personales*», si el tratamiento implica una cantidad considerable de datos personales y un gran número de partes interesadas[1481]. Esto subraya "la necesidad de una protección dinámica de la protección de datos personales en la que el interesado desempeña un papel cada vez más activo en la dinámica relativa al tratamiento de datos personales".

86. El Capítulo IV del RGPD se dedica al "Responsable del tratamiento y encargado del tratamiento", y en el mismo se indica en detalle las tareas y funciones, destinadas a garantizar la seguridad de los datos personales, sobre los individuos. El «*responsable*» es la «*persona física o jurídica*», la «*autoridad pública*», el «*servicio*» u «*otro organismo*» que, individualmente o junto con otros, determina los fines y los medios del tratamiento de los datos personales[1482]. En particular, se exige al responsable del tratamiento que establezca «*medidas técnicas y organizativas apropiadas*», que se revisarán y actualizarán cuando sea necesario, «*a fin de garantizar y poder demostrar que el tratamiento es conforme*» con el RGPD[1483]. Esas medidas «*deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y las libertades de las personas físicas*» (considerando 74). Para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento se mencionan expresamente la «*adhesión a códigos de conducta o a un mecanismo de certificación*»[1484].

87. Este nuevo enfoque es uno de los elementos más importantes en el nuevo marco regulatorio, ya que expresa claramente la responsabilidad proactiva ("*accountability*") de los responsables en relación con los tratamientos que realizan. El principio de "*accountability*" se constituye como uno de los pilares fundamentales del RGPD tal y como se describe claramente en su considerando 74[1485]. Se trata de que el responsable del tratamiento esté

[1481] Considerando 75 del RGPD.
[1482] Según el artículo 4, núm. 7, del RGPD el «*responsable del tratamiento*» o «*responsable*» es «*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros*».
[1483] Artículo 24 (Responsabilidad del responsable del tratamiento), apartado 1, del RGPD. *Vid*. en particular, Simone CALZOLAIO (2017), «Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679», en *federalismi.it*, núm. 24, págs. 12 y ss. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35361 [consulta: 23 de diciembre de 2017].
[1484] Artículo 24, apartado 2, del RGPD. Sobre los códigos de conducta o a un mecanismo de certificación, *vid*. artículos 40 y 42 del mismo Reglamento
[1485] Considerando 74 del RGPD: «*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el*

«*obligado a aplicar medidas oportunas y eficaces*» y pueda demostrar el cumplimiento de las actividades de tratamiento con el RGPD, «*incluida la eficacia de las medidas*». Estas medidas deberían «*tener en cuenta la naturaleza, el ámbito, el contexto y los fines del trato, así como el riesgo para los derechos y las libertades de las personas físicas*». Así, como señala el artículo 5 del RGPD, el responsable del tratamiento deberá tratar los datos de manera «*responsable*» y deberá ser capaz de demostrarlo. De hecho, los responsables no sólo deben «*garantizar el cumplimiento de las disposiciones del Reglamento*»[1486], sino también demostrar adecuadamente cómo garantizan dicho cumplimiento.

88. El nuevo Reglamento aborda muy cuidadosamente los problemas de las medidas de seguridad que deben aplicarse, y presta atención particular a la evaluación y la gestión de los riesgos, con el fin de proporcionar una protección efectiva de forma preventiva y no sólo *a posteriori* de posibles abusos con respecto al tratamiento de datos. En virtud del RGPD se menciona una nueva obligación de «*protección de datos desde el diseño*»[1487] ("*data protection by design*") y «*protección por defecto*» ("*by default*"), requiriendo – dada «*la tecnología disponible y el coste de la aplicación*» y «*la naturaleza, ámbito, contexto y fines del tratamiento*», así como «*la probabilidad y gravedad*» de los riesgos derivados del tratamiento de los derechos y libertades de las personas – la adopción de «*medidas técnicas y organizativas apropiadas*» para aplicar efectivamente los principios de protección de datos, como la seudonimización[1488] y minimización de datos, a fin de «*cumplir los requisitos*

responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas».

[1486] Considerando 81 del RGPD.

[1487] Sobre los antecedentes internacionales y europeos del nuevo principio y obligación, *amplius* Miguel RECIO GAYO (2017a), «Protección de Datos desde el Diseño: principio y obligación en el RGPD», en *Lefebvre - El Derecho*, 20.02.2017. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/Proteccion-Datos-Diseno-obligacion-RGPD_11_1057930001.html. El legislador europeo ha transladado efectivamente el concepto de "*privacy by design*" en el Reglamento, que circuló en el debate internacional desde hace tiempo. En particular, el mérito de la intuición original se atribuye principalmente a Ann Cavoukian, que ocupó el cargo de *Information and Privacy Commissioner de Ontario* (Canadá). En este sentido, para una elaboración conceptual de los principios subyacentes a la noción de "*privacy by design*", véase Ann CAVOUKIAN (2010), «Privacy by design: the definitive workshop. A foreword», en *Identity in the Information Society*, vol. 3, issue 2, págs. 247-251. Disponible en Internet: https://link.springer.com/article/10.1007/s12394-010-0062-y.; y siempre de la misma autora, «Privacy by Design. Strong Privacy Protection - Now, and Well into the Future», *A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners*, 2011, págs. 35. Disponible en Internet: https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf [documentos consultados: 27 de marzo de 2017].

[1488] Sobre la seudonimización, *vid. supra*. Recordamos que la seudonimización es muy diferente de la técnica de anonimización de datos: de hecho, los datos que se han convertido en anónimos ya no se consideran datos personales y, como tales, no están sujetos a regulación, debido a los medios disponibles y los costes relacionados que el procedimiento de anonimización implica, es muy difícil identificar a la persona en cuestión; por lo contrario, el dato seudonimizado es en general un dato que siempre se trata de forma anónima, pero de

del presente Reglamento y proteger los derechos de los interesados»[1489]. Esto, con el fin de salvaguardar los derechos del responsable del tratamiento y garantizar, entre otras cosas, que sean tratados, por defecto, sólo los datos personales necesarios para cada propósito específico del tratamiento[1490].

89. En particular, el principio de protección de datos desde el diseño tiene carácter horizontal y tiene como objetivo garantizar el cumplimiento de las reglas básicas de la disciplina a lo largo del ciclo de vida de la información personal, ya que como se indica en dicho considerando «*el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto*». Los «*principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos*», de manera que sea un requisito o condición exigible en la adquisición de productos o servicios por las autoridades públicas[1491].

---

acuerdo con modalidades que, cuando es necesario, hacen que sea fácil identificar a la persona a quien se refiere. *Vid*. Franco PIZZETTI (2016b: 257); Cedric BURTON, Laura DE BOEL, Christopher KUNER, Anna PATERAKI, Sarah CADIOT and Sára G. HOFFMAN (2016), «The Final European Union General Data Protection Regulation», en *Bloomberg Law: Privacy & Data Security*, February 12. Disponible en Internet: https://www.bna.com/final-european-union-n57982067329 [consulta: 27 de marzo de 2017].

[1489] Artículo 25 (Protección de datos desde el diseño y por defecto), apartado 1, del RGPD. Con referencia a los requisitos necesarios para la transferencia de datos, artículo 47 de las "Normas corporativas vinculantes" y el considerando 108.

[1490] Artículo 25, apartado 2, del RGPD: «*El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas*». Para identificar la esencia del principio de "protección de datos por defecto", *vid*. EUROPEAN COMMISSION - Directorate-General Justice, Freedom and Security (2010: 51); y EDPS (2012: 29); Christopher KUNER (2012), «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law», en *Bloomberg BNA Privacy and Security Law Report*, págs. 12. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781 [consulta: 28 de marzo de 2017].

[1491] Considerando 78 del RGPD. Por protección de datos desde el diseño y por defecto nos referimos a modelos de diseño preestablecidos de acuerdo con fórmulas estándar, y de conformidad con los criterios establecidos por ley, a los que cada responsable del tratamiento debe cumplir para que el tratamiento pueda considerarse lícito. La adopción de la protección desde diseño significa que antes de procesar cualquier trato de datos, ya se tienen en cuenta los perfiles de privacidad y protección de los datos personales de los interesados, lo que permite elaborar la mejor estrategia de organización y técnica según el tipo de tratamiento, sin tener que esperar a que se produzca algún "problema técnico" para poder configurar las medidas de seguridad pertinentes a aplicar. De hecho, la protección desde diseño desempeña su función principal en la preparación y planificación de las actividades de tratamiento, donde las medidas técnicas y organizativas son predeterminadas por el responsable y posteriormente restringidas para respetar efectivamente los principios relativos a la protección de los datos personales. De lo contrario, la protección por defecto opera en un momento posterior y se refiere específicamente a los métodos y soluciones técnicas establecidas por el responsable a través de configuraciones predefinidas correspondientes a los aspectos cuantitativos y cualitativos de la recopilación, la duración de la conservación, los propósitos del tratamiento y accesibilidad a los datos para que la configuración predeterminada de los sistemas de seguridad pueda garantizar que no se produzcan daños graves a las personas involucradas.

90. Por ello, para integrar el tratamiento con las garantías necesarias, dispuestas por las disposiciones reglamentarias y proteger los derechos de los sujetos involucrados, el responsable no puede ignorar los principios que subyacen al tratamiento: el principio de la "finalidad" de los datos «*recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*»; la "minimización de datos" que requiere que sean «*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*»; o el principio de "conservación" de datos «*mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales*»; y por último el principio de "integridad y confidencialidad" por el cual los datos serán «*tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas*»[1492].

91. Por consiguiente, la protección de datos desde el diseño, como se ve, está sujeta a controles y evaluación sobre la base de estándares de razonabilidad y proporcionalidad que requieren adopción de medidas variables dependiendo de la relevancia de factores tales como naturaleza, finalidad, contexto de tratamiento y riesgos que puede derivar[1493]. Por el contrario, en lo que respecta a la protección por defecto, el responsable debe adoptar las medidas técnicas y organizativas adecuadas para que, de forma predeterminada, sólo se traten los datos necesarios para cada finalidad específica (principios de finalidad y minimización), evitando el peligro de que los datos personales sean accesibles a un número indefinido de personas, sin intervención directa por parte del interesado.

92. La minimización de datos personales refleja la intención del legislador europeo de hacer la protección mucho más rigurosa: los datos tendrán que ser «*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*»[1494]. La minimización, que se distingue de la seudonimización, consiste en la recopilación de datos sólo pertinentes y se limita a lo que es necesario con respecto a los fines para los que se procesan. Esta técnica de "sustracción", llevada a sus consecuencias extremas, conduce a la

[1492] *Vid*. artículo 5, apartado 1, del RGPD.
[1493] Demetrius KLITOU (2014), *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, T.M.C. Asser Press, págs. 338.
[1494] Artículo 5 (Principios relativos al tratamiento), apartado 1, letra c) del RGPD. *Cfr. supra* en particular, Simone CALZOLAIO (2017: 12 y ss.).

anonimización de los datos, que se configura como un tratamiento que tiene como objetivo evitar la identificación de la persona en cuestión. Los datos anónimos no entran dentro del alcance de la nueva legislación de protección de datos.

93. En síntesis, los artículos 24 y 25 del nuevo RGPD obligan al responsable del tratamiento a adoptar medidas técnicas y organizativas adecuadas para garantizar, desde la fase de diseño, la protección del individuo, mientras que al mismo tiempo se ofrece a la comunidad un conjunto de información "residual" útil para fines de interés colectivo. Este es un principio global que, mediante la protección de la autodeterminación de la información personal, se presta también a la protección de grupos, territorios y Estados: una necesidad especialmente sentida en el continente europeo, en el momento de la elaboración de perfiles y la vigilancia masiva por razones de seguridad pública.

94. El legislador europeo parece optar por un enfoque basado no en la reparación del ilícito, sino en la prevención del daño; esto también se confirma por el hecho de que la disposición carece de una lista exhaustiva de las tareas y actividades que el responsable del tratamiento de datos debe establecer, sino más bien del análisis del riesgo y de cualquier daño causado. Así que, "la protección de los derechos y libertades de las personas en lo que respecta al tratamiento de datos personales requiere la adopción de medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de las disposiciones del RGPD". Para demostrar este cumplimiento, el responsable del tratamiento de datos «*debe adoptar políticas internas y aplicar medidas*» que, en particular, cumplan los principios de "protección de datos desde el diseño" y la "protección de datos por defecto" (considerando 78). De hecho, en los últimos tiempos ha surgido un debate amplio y complejo, tanto en la opinión pública y entre los juristas, sobre la cuestión de la legitimidad de los sistemas de seguridad, cuando se convierten en un obstáculo a la protección frente a las amenazas contra la seguridad pública y la justicia, lo que lleva a cuestionar el alcance que deben tener las obligaciones a los productores de dispositivos para ayudar a las autoridades policiales a la resolución de actos terroristas, que, en última instancia, son mecanismos que garantizan la privacidad[1495]. Este debate se está desarrollan en el plano internacional y, en ese contexto,

[1495] Por ejemplo, nos referimos al cifrado preparado por *Apple* en sus dispositivos móviles. El asunto nació de la disputa que ha visto contrapuestos el gobierno de EE.UU. y la empresa *Apple*. Todo nació después de la matanza en el centro social para personas discapacitadas en San Bernardino, California, el 2 de diciembre de 2015 por obra de Syed Farook y Tashfeen Rizwan Malik, marido y mujer, que abrieron fuego contra la multitud, matando a 14 personas y heridas a otras 23, incluidos dos policías. Posteriormente, los dos atacantes fueron asesinados en un enfrentamiento con la policía. Más allá de la crónica, el hecho también tuvo notable resonancia a nivel jurídico, a causa de la solicitud del *FBI* a *Apple*, basada en una orden impuesta a *Apple* por

se enriquece la contribución europea, y está lejos de resolverse, auque lo que no parece concebible ni deseable es que cada Estado establezca normas nacionales en un sector altamente globalizado[1496].

95. El Reglamento señala expresamente el cifrado entre las herramientas esenciales para proteger a las personas y entre las medidas técnicas adecuadas para garantizar "un nivel adecuado" de seguridad en el tratamiento de datos. Con el cifrado el responsable o el encargado, «*a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto del Reglamento*», deben «*evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos*»[1497]. El artículo 32 titulado "Seguridad del tratamiento" abre la Sección II del Capítulo IV sobre seguridad de los datos del RGPD. También en esta disposición se reitera la obligación general del responsable y encargado del tratamiento de aplicar «*medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. seguridad apropiada al riesgo*». Una vez más, se establece una obligación técnico-organizativa, previa a la ejecución del tratamiento, siempre con vistas a una protección preventiva eficiente, que para el legislador es un requisito fundamental para el correcto tratamiento. Esta obligación se rige principalmente en consideración de algunos requisitos, todos relacionados con el tratamiento, que se deben investigar cuidadosamente antes de comenzar el proceso en sí, con el fin de minimizar, si no eliminar por completo, los riesgos asociados con la actividad de tratamiento: «*el estado de la técnica, los costes de aplicación,*

un juez federal del distrito central de California Sheri Pym, para instalar un software que "descifre" los contenidos del *iPhone* de uno de los autores de la masacre de San Bernardino. *Apple* rechazó la petición del *FBI* con la explicación de que al aceptar la solicitud habría creado un "precedente peligroso". Luego el *iPhone* fue desbloqueado autónomamente por el *FBI* sin la cooperación de *Apple*. En relación con la disputa en las principales bases de la regulación en apoyo de las diversas posiciones y las cuestiones legales que originaron el litigio, y sobre las posibles implicaciones del modelo de "descifrado coercitivo", *vid*. Giorgio RESTA (2016), «Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza», en *Etica ed Economia*. Disponible en Internet: http://www.eticaeconomia.it/il-caso-usa-v-apple-e-il-dilemma-dei-diritti-nella-societa-della-sorveglianza/. También se vea la interesante entrevista del SEPD sobre la pelea entre *Apple* y el *FBI* bajo el título «Apple contra el FBI: la delgada línea entre privacidad y seguridad pública», en *Euronews*, 02/03/2016. Disponible en Internet: http://es.euronews.com/2016/03/02/apple-contra-el-fbi-la-delgada-linea-entre-privacidad-y-seguridad-publica [documentos consultados: 26 de marzo de 2017].

[1496] Un ejemplo de esta tendencia se produjo en el Reino Unido cuando el ex Primer Ministro David Cameron, unos pocos días después de los ataque en París, prometió nuevas medidas contra el terrorismo, que prohibirían precisamente el uso de aplicaciones para teléfonos inteligentes como el famoso *WhatsApp* (pero también aplicaciones como come *iMessage*, *Telegram*, *Cyberdust*), ya que no permite que los servicios de seguridad lean los mensajes privados de los ciudadanos con el fin de mantener a las mismas personas seguras, y del poder de las autoridades policiales para censurar un sitio web sin tener que pedir el autorización del juez. En «Cameron plantea prohibir WhatsApp en Reino Unido tras los ataques en París», en *Diario ABC*, 13/01/2015. Disponible en Internet: http://www.abc.es/internacional/20150113/abci-cameron-whatsapp-kouachi-201501131107.html [consulta: 26 de marzo de 2017]. Las reformas propuestas por Cameron son parte de una nueva legislación para obligar a los operadores de telecomunicaciones y proveedores de servicios de Internet a almacenar información acerca de las actividades en línea de las personas, incluidos los mensajes de redes sociales (*Investigatory Powers Bill*), que ya habíamos mencionado en los capítulos anteriores.

[1497] Considerando 83 del RGPD.

y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas» (artículo 32).

96. Entre las nuevas obligaciones a cargo del responsable del tratamiento, para mejorar el cumplimiento del Reglamento cuando el tratamiento pueda presentar «*un alto riesgo para los derechos y libertades de las personas físicas*», el responsable debería realizar una evaluación del impacto de la protección de datos para determinar, «*en particular, el origen, la naturaleza, la particularidad y la gravedad de este riesgo*»[1498]. La evaluación de impacto en la protección de datos personales (EIPD) es una técnica que se ha utilizado durante mucho tiempo y que puede abordar tanto los tratamientos considerados individualmente como la agregación e interacción en todos sus tratamientos relacionados con la misma información. Su principal objetivo es reducir los riesgos para la protección de los datos personales y para otros derechos que puedan verse afectados como consecuencia del tratamiento de los datos de carácter personal. En consecuencia, el análisis de los riesgos y la medición de éstos es una parte importante de toda evaluación de impacto. Sin embargo, no es la única y, además, en el caso de la evaluación de impacto, el análisis de riesgos debe llevarse a cabo con ciertas particularidades que lo distinguen de otro tipo de análisis de riesgos cuya realización podría ser conveniente también para la organización.

97. De acuerdo con el artículo 35 (Evaluación de impacto relativa a la protección de datos), apartado 1, la obligación del responsable del tratamiento de realizar, antes del tratamiento, la «*evaluación de impacto*» generalmente existe cuando se aplica el tratamiento, especialmente cuando implica el uso de nuevas tecnologías y teniendo en cuenta su «*naturaleza, alcance, contexto o fines*» «*entrañe un alto riesgo para los derechos y libertades de las personas físicas*». La norma enumera las hipótesis particulares en las que se requiere una evaluación de impacto, principalmente relacionada a la «*evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles,* (…) *tratamiento a gran escala de las categorías especiales de datos* (…)*, u observación sistemática a gran escala de una zona de acceso público*»[1499]. Cuando la evaluación del impacto de la protección de datos

[1498] Considerando 84 del RGPD.

[1499] Artículo 35, apartado 3, del RGPD. El SEPD, aunque comparte el sistema general de la norma, ha criticado la referencia a tratamientos «*a gran escala*», considerando que este concepto es ambiguo y desatiende el hecho de que los riesgos elevados también pueden ser inherentes a los tratamientos llevados a cabo a pequeña escala, por la naturaleza particular de los datos u otras características del procesamiento. El mismo ha especificado

indica que el tratamiento tiene «*un alto riesgo que el responsable no puede mitigar*» mediante medidas apropiadas «*en términos de tecnología disponible y costes*» de implementación, se debe consultar a la autoridad de supervisión antes del tratamiento[1500].

98. Aunque no existe una definición de "evaluación de impacto", se enumeran los requisitos mínimos y, por lo tanto, debe contener necesariamente una descripción sistemática de los tratamientos previstos y la finalidad prevista, incluido «*el interés legítimo perseguido por el responsable*»; «*una evaluación de la necesidad y proporcionalidad*» de los tratamientos en relación con las finalidades; «*una evaluación de los riesgos para los derechos y libertades de los interesados*», de conformidad con las disposiciones del apartado 1 del artículo 35 y, por último, «*las medidas previstas*» para enfrentar «*los riesgos, incluidas garantías*» y mecanismos de seguridad «*para la protección de los datos personales y los derechos y libertades fundamentales*», que demuestrae el cumplimiento del tratamiento con la legislación europea[1501]. Ulteriormente, las directrices del Grupo de Trabajo[1502] aclaran que la evaluación de impacto no siempre es obligatoria, sino es únicamente obligatoria cuando el tratamiento "puede dar lugar a un alto riesgo de los derechos y libertades de personas físicas". En los casos en los que no esté claro si se requiere una evaluación de impacto, el Grupo recomienda realizar una, ya que esta evaluación representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos. Aunque en otras circunstancias pueda requerirse una evaluación de impacto, el artículo 35, apartado 3, ofrece algunos ejemplos de cuando una operación de tratamiento «*es probable que entrañe un alto riesgo*»[1503].

---

que la lista mencionada en el apartado 3 tiene carácter esemplificativo y no puede considerarse exhaustiva de todas las hipótesis en las que recurren las condiciones para llevar a cabo una evaluación de impacto. EDPS (2012: 32-33).

[1500] Artículo 36, apartado 1, del RGPD. Ese alto riesgo puede surgir de ciertos tipos de procesamiento y del alcance y frecuencia del tratamiento, lo que también podría resultar en daño o interferencia con los derechos y libertades del individuo. La autoridad de control que recibe la «*solicitud de consulta*» debe realizar un seguimiento dentro de un período específico (ocho semanas), con «*cualquier intervención de dicha autoridad basada en las funciones y poderes*» que le atribuye el artículo 58 del Reglamento (investigación, correctivos, autorización y consultivos) incluido la facultad de prohibir el tratamiento (apartado 2). Considerando 94 del RGPD.

[1501] Artículo 35, apartado 7, del RGPD. *Vid*. Ruth BENITO MARTÍN (2017), «¿Qué es una evaluación de impacto en protección de datos?», en *Lefebvre - El Derecho*, 18.04.2017. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/Evaluacion-impacto-reglamento-proteccion-datos_11_1076305003.html [consulta: 21 de abril de 2017].

[1502] ARTICLE 29 DATA PROTECTION WORKING PARTY (2017a), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, 17/EN, WP 248 rev.01, págs. 8 y ss. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [consulta: 11 de octubre de 2017].

[1503] Las palabras «*en particular*» indicadas en la frase introductoria del artículo 35, apartado 3, del RGPD se refieren a una lista no exhaustiva. Pueden existir operaciones de tratamiento de «*alto riesgo*» que no estén incluidas en esta lista pero que supongan unos riesgos similarmente elevados. Estas operaciones de tratamiento

99. Por el contrario, no se requiere una EIPD cuando[1504]: «*no sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas*» (artículo 35, apartado 1); la naturaleza, el alcance, el contexto y los fines del tratamiento sean muy similares al tratamiento para el que se ha realizado la evaluación de impacto; las operaciones de tratamiento hayan sido comprobadas por la autoridad de control antes de mayo de 2018 en condiciones específicas que no hayan cambiado; una operación de tratamiento «*tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro*», cuando «*tal Derecho regule la operación específica de tratamiento*» y cuando ya se ha realizado una evaluación de impacto de protección de datos en el contexto de la adopción de dicha base jurídica (artículo 35, apartado 10)[1505]; el tratamiento se incluya en la lista opcional (establecida por la autoridad de control) de operaciones de tratamiento para las que no se requiere una evaluación de impacto (artículo 35, apartado 5).

100. Los nuevos instrumentos ahora considerados se basan en una evaluación cuidadosa de los riesgos de violación de los derechos y libertades fundamentales de las personas interesadas, a partir de la cual el responsable está obligado a establecer medidas y soluciones técnicas destinadas específicamente a la protección de datos personales. Se sigue un enfoque preventivo de la nueva legislación diseñada para implementar, aunque con cierta reserva, los principios de la legislación europea. Entre ellos, ocupan un papel cada vez más importante los principios de prevención y precaución cuando, sin referirse a ellos, la legislación discute «*riesgos de diversa probabilidad y gravedad que supone el tratamiento para los derechos y libertades de las personas físicas*» (artículo 25) o establece una obligación de evaluación de impacto cuando el tratamiento pueda presentar «*un alto riesgo para los derechos y libertades de las personas*»[1506].

también deben someterse a una evaluación de impacto. ARTICLE 29 DATA PROTECTION WORKING PARTY (2017a).

[1504] ARTICLE 29 DATA PROTECTION WORKING PARTY (2017a: 12-13).

[1505] *Vid. infra.*

[1506] Artículo 35 del RGPD. Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo, se deben considerar los nueve criterios siguientes: 1) evaluación personal basada en perfiles personales; 2) toma de decisiones automatizada con efectos jurídicos en las personas; 3) observación sistemática para observar, supervisar y controlar a los interesados (video vigilancia); 4) datos sensibles o datos muy personales (por ejemplo, opiniones políticas, antecedentes penales, datos personales de salud, datos financieros, documentos personales, correos electrónicos, códigos de acceso personal); 5) tratamiento de datos a gran escala (por ejemplo, duración del tratamiento, área geográfica, volumen de datos procesados en relación con la población); 6) la combinación de diferentes conjuntos de datos (por ejemplo, provenientes de diferentes bases de datos y originalmente recogidos para diferentes fines, cuya combinación excede el alcance del consentimiento original); 7) datos sobre categorías de sujetos débiles (niños, ancianos, enfermos, enfermos mentales, solicitantes de asilo); 8) uso innovador de datos y nuevas tecnologías en empresas cuyas consecuencias personales y sociales son desconocidas (por ejemplo, huellas dactilares, reconocimiento facial, Internet de las cosas); 9) cuando el tratamiento en sí mismo impide que los sujetos de los datos ejerzan un derecho o utilicen un servicio o contrato. Las operaciones de tratamiento de datos pueden

101. Todo lo señalado hasta ahora sobre la evaluación de impacto (como la "consulta previa", artículo 36) está sujeta a exenciones a favor de los Estados. De una interpretación combinadas del considerando 93 y del apartado 10 del artículo 35[1507] se deduce claramente que las entidades públicas estarán libres de este cumplimiento, si en Derecho nacional que rige «*las funciones de la autoridad pública u organismo público y que regula*» el tratamiento específico o «*el conjunto de operaciones*», los Estados miembros pueden considerar necesario llevar a cabo esta evaluación a *priori* a las actividades de tratamiento. En otras palabras, existe una mera facultad y no una obligación por parte de las autoridades públicas, remitiendo la decisión de hacer obligatoria al legislador interno la evaluación del impacto de la protección de datos si es necesario.

102. En conclusión, este nuevo cambio de perspectiva propuesto por el Reglamento, que se basa en un enfoque preventivo madurado en la última década[1508], se refiere a una responsabilidad mayor y más directa de los Estados en el tratamiento de datos de carácter personal, los que lleva a los mismos a replantear todos los procesos y procedimientos para el manejo de datos personales. Es en esta perspectiva que las autoridades competentes estarán obligadas a adoptar un enfoque sistemático y estratégico para garantizar una protección eficaz de su patrimonio informativo y sistemas para preservar los datos. Por ejemplo, la introducción de los principios de privacidad desde el diseño y la privacidad por

cambiar y evolucionar en plazos ajustados, creándose nuevos riesgos y vulnerabilidades para la protección de datos. Por esta razón, la evaluación de impacto debe renovarse de acuerdo con los cambios en los tratamientos. ARTICLE 29 DATA PROTECTION WORKING PARTY (2017a: 9-11). *Vid*. Roger CLARKE (2009), «Privacy impact assessment: Its origins and development», en *Computer Law & Security Review*, vol. 25. Disponible en Internet: http://www.rogerclarke.com/DV/PIAHist-08.html. En particular, véase David WRIGHT (2012), «The state of the art in privacy impact assessment», en *Computer Law & Security Review*, vol. 28, págs. 54-61. Disponible en Internet: https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wright-2012e.pdf [documentos consultados: 22 de abril de 2017].

[1507] Artículo 35, apartado 10, del RGPD: «*Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento*».

[1508] El núcleo de la Directiva 95/46/CE era insuficiente porque se basaba en un enfoque esencialmente reparador. Este planteamiento parte de que el tratamiento de datos personales debe considerarse una actividad de riesgo, de la cual se desprende como corolario necesario la necesidad de examinar cuidadosamente la serie de riesgos relacionados con las diversas actividades de tratamiento, con el fin de garantizar una protección más completa y eficiente de los datos personales de las personas. *Vid*. ARTICLE 29 DATA PROTECTION WORKING PARTY (2014c), Statement on the role of a risk-based approach in data protection legal frameworks, Adopted on 30 May 2014, 14/EN, WP 218.

defecto significa que cada tratamiento debe respetar el principio de estricta necesidad, finalidad, y garantizar el pleno ejercicio de los derechos del interesado[1509].

3.2. Exclusiones y limitaciones en el RGPD: cómo los Estados pueden exceder los principios y reglas de privacidad

103. Para comprender mejor los elementos claves de la normativa europea en materia de protección de datos, se debe prestar una especial atención a la "delimitación del ámbito de aplicación material del RGPD", en el que se hace referencia a que los aspectos relacionados con la «*protección y prevención frente a las amenazas a la seguridad pública podrían tener un tratamiento diferente*»[1510].

104. Por consiguiente, si las instituciones de la UE han diseño una norma como el RGPD, de aplicación directa y obligatoria en todas sus partes, con mayor exhaustividad y claridad en su contenido y disciplinando en la manera más precisa posible la materia[1511], si todo esto es cierto ¿por qué el texto del RGPD atribuye tantos poderes a los Estados miembros y a las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención?

105. A tal fin, ante todo tenemos que identificar el ámbito de aplicación material del nuevo Reglamento, que se puede distinguir en dos. El artículo 2, apartado 1, podemos decir que delinea en positivo el ámbito de aplicación material[1512], no muy diferente de la disposición ya contenida en la Directiva 95/46/CE, en sentido de que el RGPD se aplica «*al*

[1509] Estas obligaciones parecen también aplicarles a los fabricantes de dispositivos y sistemas operativos, como especifica el Grupo de Trabajo en su opinión 02/2013, sobre las aplicaciones para dispositivos inteligentes. ARTICLE 29 DATA PROTECTION WORKING PARTY (2013b), Opinion 02/2013 on apps on smart devices, Adopted on 27 February 2013, 00461/13/EN, WP 202. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf [consulta: 23 de abril de 2017].

[1510] Así se expresó Rafael García Gonzalo, jefe del Departamento Internacional de la Agencia Española de Protección de Datos (AEPD), durante el VIII Foro de la Privacidad organizado por el Data Privacy Institute (DPI) de ISMS Forum Spain, el 12 de febrero en Madrid. En «Conclusiones VIII Foro de la Privacidad del Data Privacy Institute», en *Lefebvre - El Derecho*, Madrid, 17.02.16.

[1511] En consecuencia, hace falta una consideración importante. A menudo, el contenido de un reglamento de la UE es un compromiso político, sobre todo por la complejidad de la materia a tratar, como ocurre con el tratamiento de los datos y la seguridad. Por esta razón, el RGPD representa una amplia legislación marco que, en algunas áreas específicas, ha dado deliberadamente a los legisladores nacionales y a las autoridades competentes el poder de intervenir para garantizar que despliegue concretamente sus efectos.

[1512] Maria Gabriella STANZIONE (2016), «Il nuovo regolamento europeo sulla protezione dei dati personali: genesi e ambito di applicazione», en *Comparazione e Diritto Civile*, giugno, pág. 9. Disponible en Internet: http://www.comparazionedirittocivile.it/prova/files/Stanzione_MG_Genesi_Ambito_Applicazione_Comparazione_2016.pdf [consulta: 25 de abril de 2017].

tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero»[1513]. Estas simples líneas con las que traza el ámbito de aplicación material, tienen implicaciones importantes para el análisis que a continuación se va a desarrollar.

106. En primer lugar, el concepto de «*datos personales*» se amplía en relación con la información que identifica o hace que la persona física sea identificable («*el interesado*»). La protección otorgada por el RGPD «*debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales*» (considerando 14). Se considera que una persona es "identificable"[1514], a través de una ampliación de la categoría de identificadores que, además de las tipologías clásicas – como por ejemplo el nombre, el número de identificación y los elementos característicos de la identidad física, fisiológica, psíquica, económica, cultural y social – se añaden nuevos tipos de identificadores estrechamente vinculados a las tecnologías desarrolladas en los últimos años: datos de localización (piense en los datos transmitidos por dispositivos de *GPS*), identificadores en línea o elementos que son característicos de la identidad genética de una persona[1515]. Debe tenerse en cuenta la trascendencia de este

[1513] Aunque la norma mencionada reproduce el texto del artículo 3, apartado 1, de la Directiva de 1995, la comparación entre las definiciones de "datos personales" y "tratamiento" en los dos actos legislativos revela algunas importantes diferencias. *Cfr*. artículo 3 (Ámbito de aplicación), apartado 1, de la Directiva 95/46/CE: «*Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*».

[1514] El artículo 4, núm. 1, del RGPD no define más el concepto de datos personales, que sigue siendo bastante ambiguo si se refiere únicamente al texto del dispositivo, donde las indicaciones interpretativas pueden encontrarse en los considerandos: el considerando 26 declara que, para determinar si una persona física es identificable, «*deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física*». También se especifica que las personas pueden ser asociadas con identificadores en línea proporcionados por sus dispositivos, «*como direcciones de los protocolos de internet, identificadores de sesión en forma de cookies u otros identificadores, como etiquetas de identificación por radiofrecuencia*». *Vid*. considerando 30 del RGPD. Tal como surgió en su opinión el Grupo de Trabajo, la noción de datos personales aceptada por la Directiva 95/46/CE ha generado diferentes interpretaciones en los sistemas jurídicos europeos. ARTICLE 29 DATA PROTECTION WORKING PARTY (2007), Opinion 4/2007 on the concept of personal data, Adopted on 20th June, 01248/07/EN, WP 136. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [consulta: 25 de abril de 2017].

[1515] Debe entenderse por «*datos genéticos*» los datos personales «*relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona*»; por «*datos biométricos*» los datos personales «*obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*». Artículo 4, apartados 13-14 y considerando 34 del RGPD. En el sistema de definiciones, el Reglamento, por primera vez, introduce dos categorías de datos pertenecientes a la esfera biológica y genética de la persona: categorías de datos que, en ciertos sectores y mediante el uso de ciertas tecnologías (como las que permiten el uso de escáneres faciales biométricos o estudios fotográficos particularmente intrusivos), son particularmente susceptibles de violaciones importantes en términos de privacidad, protección de datos personales y, tal vez, más en general,

significado, ya que la noción de datos personales es el pivote alrededor del cual gira toda la normativa, trazando los límites de la aplicación de la misma, por lo que intervenir en un sentido restrictivo o extensivo sobre la definición de datos personales significa afectar significativamente el alcance de la legislación.

107. Por otra parte, el nuevo RGPD aumenta significativamente la lista de operaciones que, de forma individual o conjunto, ya sea por procedimientos automatizados o no, constituyen un «*tratamiento*» de datos personales, como: «*recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*»[1516]. Se agrega una nueva operación como es la «*limitación del tratamiento*», cuya definición se expresa en el siguiente número y que, en particular, consiste en un «*marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*»[1517]. El interesado tiene derecho a obtener del responsable del tratamiento de datos la limitación del procesamiento cuando se produce una de las siguientes hipótesis: el interesado cuestiona la exactitud de los datos personales, durante el período necesario para que el responsable del tratamiento verifique la exactitud de dichos datos personales; el tratamiento es ilícito y el interesado se opone a la cancelación de datos personales y, en cambio, pide que su uso sea limitado; aunque el responsable de datos ya no lo necesita para fines de procesamiento, los datos personales son necesarios para que el interesado investigue, ejerza o defienda un derecho ante un tribunal; la parte interesada se opuso al tratamiento de conformidad con el artículo 21, apartado 1[1518], a la espera de la verificación de la posible prevalencia de los motivos legítimos del responsable del tratamiento de datos con respecto a los de la parte interesada[1519]. Pero, cuando el tratamiento se limita a las hipótesis ahora mencionadas, dichos datos personales sólo se tratarán, con excepción del almacenamiento, con el consentimiento del interesado o para el establecimiento, ejercicio o defensa de reclamaciones legales o para la protección de

de libertad de autodeterminación. Lo que es propio de esta categoría de datos parece residir más bien en su idoneidad para permitir la identificación unívoca de la persona.

[1516] Artículo 4, núm. 2, del RGPD.

[1517] Artículo 4, núm. 3, del RGPD.

[1518] Artículo 21 (Derecho de oposición), apartado 1: «*El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones*».

[1519] Artículo 18, apartado 1, del RGPD.

los derechos de otro natural o persona jurídica o por razones de interés público importante de la Unión o de un Estado miembro.

108. Constituye una novedad ulterior la definición de «*elaboración de perfiles*» (en inglés, "*profiling*"), que se refiere a cualquier forma de procesamiento automatizado de datos personales consistente en utilizar datos personales para «*evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*»[1520]. El fenómeno de la elaboración de perfiles plantea muchos temores, ya que representa una forma de tratamiento de datos personales con un alto potencial invasivo para los derechos fundamentales del individuo. Según el artículo 22 del RGPD, el interesado «*tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*». Pero el segundo apartado prevé una cláusula de no aplicación si la decisión «*a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado*»[1521].

109. En una primera observación, el "*profiling*" consiste en un proceso de elaboración de información, que se extrae de las bases de datos, para crear perfiles extremadamente

[1520] Artículo 4, núm. 4, del RGPD. *Vid*. también el considerando 71 del mismo Reglamento: «*Este tipo de tratamiento incluye la «elaboración de perfiles» consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar*».

[1521] Artículo 22, apartado 3 y 4: «*En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado*». El único antecedente directo con la elaboración de perfiles se puede encontrar en el artículo 15 de la Directiva 95/46/CE, que tenía una relación similar, sin mencionar las técnicas de elaboración de perfiles. *Cfr*. artículo 15 (Decisiones individuales automatizadas), apartado 1, de la Directiva 95/46/CE: «*Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.*».

detallados de la persona o grupo en cuestión. La elaboración de perfiles se aplica luego a las personas y se colocan sobre la base de las decisiones que se tomarán con respecto a ellos. La elaboración de perfiles permite, de hecho, presumir una serie de características individuales, a la luz de otros aspectos ya conocidos por el mismo individuo o su grupo de pertenencia. A través de la elaboración de perfiles, se conocen aspectos, elementos y correlaciones del sujeto perfilado que no sería posible extraer a través de los métodos clásicos de análisis. Por lo tanto, la elaboración de perfiles no sólo produce información, sino que genera una nueva etapa de conocimiento, a través de la cual es posible observar y predecir comportamientos, actitudes y preferencias de forma analítica (es decir, de perfil). El perfil demuestra ser un medio funcional para la asunción de una decisión relevante para el individuo o para el grupo perfilado, precisamente porque es adecuado para «*analizar o predecir*» "analíticamente" el comportamiento presente y futuro del interesado[1522].

110. La elaboración de perfiles, si no es gestionada y controlada de forma específica, puede provocar problemas muy graves para la protección de los datos personales[1523], ya que un uso desconsiderado, indiscriminado y generalizado de esta técnica pueda permitir un control global y constante del comportamiento de la población por parte de las autoridades públicas, afectando negativamente a aspectos de la vida privada de personas particularmente sensibles. Al recopilar datos de diferentes fuentes, las autoridades estatales pueden formar perfiles personales sobre los individuos. Estos perfiles pueden revelar hechos sensibles y usarse para predecir acciones futuras y categorizar a alguien como riesgo. Esta recopilación de datos a gran escala presenta múltiples riesgos ya que personas no autorizadas podrían hacer uso de esos datos y, en este sentido, diferentes centros de datos gubernamentales han sido pirateados y los gobiernos se espían entre sí. El problema serio es la incapacidad del

[1522] Como se destaca en los estudios de Mireille Hildebrandt, la esencia del proceso en cuestión radica en hacer visible lo que es imperceptibles a simple vista, con el fin de permitir el análisis predictivo de las conductas y preferencias individuales. *Vid*. Mireille HILDEBRANDT (2009), «Who is Profiling Who? Invisible Visibility», en Serge GUTWIRTH, Yves POULLET, Paul DE HERT and others (eds.), *Reinventing Data Protection?*, Dordrecht, Springer, págs. 239-252. Disponible en Internet: https://www.researchgate.net/publication/226541992_Who_is_Profiling_Who_Invisible_Visibility. Sobre este tema es muy útil profundizar a través de la investigación *Profiling. Protecting citizens' rights fighting illicit profiling*, project funded by the European Commission, DG Justice, under the Fundamental Rights and Citizenship programme, 2014, págs. 192. Disponible en Internet: http://www.unicri.it/news/files/Profiling_final_report_2014.pdf [documentos consultados: 27 de abril de 2017].

[1523] En este sentido, «EDRi's suggested amendments to the Commission's. Proposal for a Regulation on the Protection of individuals with regard to the processing of personal data, and the free movement of such data (General Data Protection Regulation) COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)», en *European Digital Rights (EDRi)*, 12/12/2012, pág. 72. Disponible en Internet: http://protectmydata.eu/topics/edris-proposed-amendments/ [consulta: 27 de abril de 2017].

individuo para controlar cómo se utilizan sus datos. El uso de datos de vigilancia es un problema de desequilibrio de poder[1524].

111. La delimitación en "negativo" del ámbito de aplicación material[1525] del RGPD se lleva a cabo en el artículo 2 del RGPD con una serie de supuestos que están excluidos del ámbito de aplicación, y así se dispone que el RGPD «*no se aplica*», en particular, al tratamiento de datos personales «*a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;* (…) *d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención*».

112. Este apartado, en particular la letra d), es importante para el alcance de la normativa europea[1526]. Este debe ser interpretado atendiendo a los considerandos 16 y 19, que excluyen del ámbito de aplicación del RGPD la protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con «*actividades relativas a la seguridad nacional*», no comprendidas del ámbito de del Derecho de la Unión. Tampoco se aplica el RGPD «*al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión*» (considerando 16). Mas concretamente, el RGPD no debe aplicarse a las actividades de tratamiento de datos de carácter personal «*por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención* (…)», en cuánto se encuentra sometidos al ámbito de aplicación de la

[1524] Niklas VAINIO (2016), «Fundamental rights compliance and the politics of interpretation: Explaining Member State and court reactions to Digital Rights Ireland», en Tobias BRÄUTIGAM and Samuli MIETTINEN, *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, pág. 252.
[1525] Maria Gabriella STANZIONE (2016: 11).
[1526] *Cfr*. artículo 3, apartado 2, de la Directiva 95/46/CE: «*Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: - efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal* (…)».

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo (*vid*. *infra*). En este ámbito se reconoce una amplia autonomía a los legisladores nacionales, que pueden «*mantener o introducir*» disposiciones más concretas y "adoptar medidas" legales para limitar las obligaciones y derechos «*siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención*» (considerando 19).

113. La protección del orden público y de la seguridad nacional, de hecho, pertenecen a un ámbito dentro del cual los Estados miembros conservan una amplia capacidad de intervención por lo que, siempre que se respeten los requisitos del RGPD, los Estados pueden establecer a efectos internos un equilibrio específico entre las necesidades de orden público y seguridad y la protección de los datos personales, especialmente en aquellos aspectos que no estén regulados directamente bajo la legislación de la UE. En este contexto, tampoco el TJUE tendría poderes de intervención que permitan reequilibrar la estructura de los sectores interesados de los Estados miembros[1527]. De hecho, las limitadas competencias del TJUE «*en el ejercicio de sus atribuciones respecto de las disposiciones* (…) *relativas al espacio de libertad, seguridad y justicia*», implica que este «*no será competente para comprobar la validez o proporcionalidad de operaciones efectuadas por la policía u otros servicios con funciones coercitivas de un Estado miembro, ni para pronunciarse sobre el ejercicio de las responsabilidades que incumben a los Estados miembros respecto del mantenimiento del orden público y de la salvaguardia de la seguridad interior*»[1528]. Esto plantea una importante dificultad a la hora de conciliar la normativa de protección de cada Estado miembro al no contar con referencias en el Derecho de la Unión Europea. Este ámbito no regulado por la legislación de la UE, genera amplios vacíos normativos que pueden dar lugar a decisiones que conduzcan a un nivel de protección fragmentada entre los Estados miembros y, en última instancia, a una protección con los límites variables de Estado a Estado.

[1527] El nuevo artículo 67 del TFUE (antiguo artículo 61 TCE y antiguo artículo 29 TUE) pone el acento en el «*respeto de los derechos fundamentales y de los distintos sistemas y tradiciones jurídicos de los Estados miembros*» y en la garantía de «*un nivel elevado de seguridad mediante* (…) *de coordinación y cooperación entre autoridades policiales y judiciales y otras autoridades competentes*»; pero todo ello, «*sin perjuicio del ejercicio de las responsabilidades que incumben a los Estados miembros en cuanto al mantenimiento del orden público y la salvaguardia de la seguridad interior*». *Vid*. artículo 72 del TFUE (antiguo artículo 64, apartado 1, TCE y antiguo artículo 33 TUE).

[1528] Artículo 276 del TFUE.

114. Con respecto al tratamiento realizado por los tribunales y las autoridades judiciales, en tanto que resulta necesario salvaguardar la independencia y la autonomía del poder judicial, el control del respeto de la normativa en materia de protección de los datos personales se atribuye a órganos específicos dentro del mismo sistema judicial. Esencialmente se introduce una autonomía en la gestión de la privacidad en favor de los tribunales nacionales, que sustituyen a la autoridad nacional, tanto en la jurisdicción ordinaria como en la administrativa. Por lo tanto, parece que se abre la posibilidad de «*organismos específicos establecidos dentro del sistema judicial del Estado miembro*», con las tareas de sustancia similares a las autoridades nacionales de protección de datos[1529].

115. La definición del ámbito de aplicación material de las nuevas reglas de privacidad europea es tan sutil como a veces enigmática. Estos son los legados de la normativa precedente, que no hacen más que provocar incertidumbre a las personas y empresas que se verán afectadas por estas regulaciones, y al mismo tiempo favorece la creación de amplios márgenes de maniobra para los Estados.

116. Incluso el RGPD también reconoce este «*margen de maniobra para que los Estados miembros especifiquen sus normas*»[1530], incluso con respecto al tratamiento de categorías particulares de datos personales, que, «*por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales*», «*ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales*»[1531], como los "datos sensibles"[1532]. Dichos datos personales no deberían

[1529] Considerando 20 del RGPD. Aunque el RGPD «*se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del RGPD, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de éste y atender las reclamaciones en relación con tales operaciones de tratamiento de datos*».

[1530] Considerando 10 del RGPD.

[1531] Considerando 51 del RGPD.

[1532] El artículo 9 (Tratamiento de categorías especiales de datos personales) del RGPD se refiere a las categorías especiales de datos y, tras establecer en el apartado 1 la prohibición del tratamiento de determinados datos «*que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física*». A las categorías especiales de datos personales ya existentes (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, y las infracciones o condenas), se añaden los datos genéticos y los datos biométricos, cuyo tratamiento, en consecuencia, pasa a estar prohibido, con carácter general, en este caso siempre que se

estar sujetos a tratamiento, a menos que se permitiese en los casos específicos cubiertos por el RGPD, teniendo en cuenta el hecho de que el Derecho de los Estados miembros puede establecer «*disposiciones específicas*» y adecuadas de protección de datos para «*adaptar la aplicación de las normas*» del RGPD para el «*cumplimiento de una obligación legal*» o la realización de «*una misión de interés público o para el ejercicio de poderes públicos*» conferidos al responsable del tratamiento[1533]. Finalmente, es necesario subrayar que el artículo 9, apartado 4, junto con el considerando 53, deja un margen de flexibilidad a los Estados, permitiéndoles intensificar el régimen de tratamiento de datos genéticos, datos biométricos y datos de salud, mediante la adopción de normas de protección más estrictas. Esta disposición, aunque compartida en la perspectiva a proporcionar a las partes la mayor protección posible, parece entrar en conflicto con los objetivos declarados de armonización de la normativa, que subyace a la regulación general sobre protección de datos.

117. Por lo tanto, a los datos sensibles, o aquellas categorías especiales de datos más expuestos a una invasión de la esfera personal y más fácilmente utilizables de manera discriminatoria, «*además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales*» y otras normas del RGPD, «*sobre todo en lo que se refiere a las condiciones de licitud del tratamiento*» (considerando 51). Asimismo, los datos personales

lleve a cabo con el fin de identificar de forma única una persona. Son "biométricos" «*los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*». Artículo 4, apartado 14, del RGPD. Para la definición completa de "datos genéticos", *vid*. *supra*.

[1533] Considerando 51 del RGPD. El apartado 2, del artículo 9 del RGPD, exceptúa la prohibición contenida en el apartado primero para remitirse al margen de apreciación nacional en este tema, de manera que «*el apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado; c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;* (…) *e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;* (…) *j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado*».

que, por su naturaleza, sean particularmente sensibles continuarán disfrutando de una protección más amplia que aquellas categorías de datos que involucran aspectos más superficiales y menos reservados de la vida de los individuos[1534]; sin embargo, será el legislador nacional quien decida conforme a su legislación, si aplicar revisiones o enmiendas o si adoptar una normativa más próxima a lo establecido en el Reglamento europeo.

118. Por último, en lo que concierne a las autoridades nacionales competentes[1535], el RGPD establece que las decisiones de la Comisión Europea y las autorizaciones de las autoridades nacionales de control basadas en la Directiva 95/46/CE, deben permanecer en vigor[1536]. Esto significa que todas las autorizaciones emitidas por las autoridades de control en más de veinte años de actividad seguirán siendo válidas, a pesar de sus posibles conflictos con la nueva normativa europea. Por lo tanto, las abundantes decisiones de las autoridades de protección de datos personales de los Estados miembros que contienen la doctrina con las interpretaciones y comportamientos en relación con los diferentes sectores y áreas acerca de la relación entre privacidad y seguridad pública, no se verán afectadas, tal y como indica

[1534] Se prevé que el consentimiento ha de ser "explícito" para autorizar el tratamiento de datos sensibles. Se añade, por tanto, un requisito más estricto, reforzando la voluntariedad real del consentimiento puesto que el consentimiento no podrá entenderse que ha sido concedido de forma implícita mediante algún tipo de acción positiva. En definitiva, será necesario que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

[1535] El RGPD también refuerza considerablemente la «*total independencia*» de las autoridades nacionales de control (Capítulo VI - Autoridades de control independientes) que, como se señalado, constituye uno de los puntos centrales del razonamiento de la sentencia del TJUE en la sentencia *Schrems*. Recordamos que las autoridades de control ya han sido introducidas por la Directiva 95/46/CE, en su artículo 28, y se han convertido en el mecanismo básico para la aplicación y control de protección de datos en la UE en la actualidad. Volviendo al RGPD, el artículo 52, apartado 1, establece claramente que «*Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento*». Las garantías específicas están previstas en el Reglamento desde el punto de vista de las prerrogativas que garantizan el estado de independencia de la autoridad con respecto al Estado que instituyó. Este artículo muestra una clara contradicción, ya que la aplicación uniforme del RGPD no se logrará mediante el mantenimiento de la independencia absoluta de las autoridades de supervisión. De hecho, además del riesgo de decisiones divergentes que van en contra de la propia finalidad de la regulación europea, se podría alentar el "*forum shopping*" por el tratamiento de los responsables no europeos que, a pesar de las diferentes prácticas administrativas a nivel nacional, podrían optar por establecerse en un determinado Estado miembro que presente a la autoridad de control más complaciente. Sin embargo, tras la sentencia *Schrems*, en respuesta a las solicitudes del TJUE, el RGPD refuerza considerablemente los requisitos de independencia de las autoridades nacionales de supervisión y el artículo 58 del mismo, titulado a detallar con precisión los poderes, también de carácter sancionatorio, atribuido a las autoridades nacionales de control. Un punto de vista diferente del artículo 28 de la Directiva 95/46/CE, que no es más que una declaración de principios: «*Estas autoridades ejercerán las funciones que les son atribuidas con total independencia*». La nueva normativa europea establece expresamente que cada autoridad de control tiene poderes, específicamente identificados, subdivididos en: poderes de investigación, poderes correctivos y, por último, los poderes de autorización y consultivos. Sin embargo, aunque sea total y completa la independencia de las autoridades, esto no exime de la necesidad de coordinarse recíprocamente, ni de la obligación de someterse a la autoridad de la Comisión, con el fin de no frustrar la aplicación uniforme del nivel Reglamento nacional.

[1536] Considerando 171 del RGPD: «(…) *Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas*».

expresamente el RGPD. Sin embargo, el Reglamento se refiere sólo a «*las autorizaciones de las autoridades de control*»[1537], por lo que no alcanza a todo el ámbito de actividades llevadas a cabo por las autoridades, y, además, tampoco se aclara con qué efectos. Además, el Reglamento incluso no sustituirá a la Directiva 2002/58/CE relativa al tratamiento de los datos del sector de las comunicaciones electrónicas para garantizar la coherencia con el RGPD[1538].

119. En fin, resultan sorprendentes las exclusiones de la tutela de los derechos y las libertades fundamentales, las actividades de la seguridad nacional y la libre circulación de datos, lo que expone a todas las personas a mayor riesgo de violaciones por parte de los Estados miembros y otras entidades públicas o privadas legitimadas por los Estados, que, al amparo de estas normas, pueden actuar violando repetidamente el derecho a la privacidad. En concreto, este apartado nos muestra que el nuevo RGPD sigue la línea de exclusión prevista en la Directiva 95/46/CE[1539]: los Estados podrán ir más allá de los principios y reglas

[1537] Considerando 171 del RGPD.

[1538] Considerando 173 del RGPD: «*El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento*». En acto hay una propuesta de la Comisión Europea de un Reglamento sobre privacidad y comunicaciones electrónicas que tiene por objeto reforzar la confianza y la seguridad en el mercado único digital mediante la actualización del marco jurídico de la privacidad electrónica. En los últimos años, la Comisión ha iniciado un importante proceso de modernización del marco de protección de datos, que culminó con la adopción, en mayo de 2016, del nuevo RGPD. La legislación *ePrivacy* debe adaptarse para alinearse con estas nuevas normas. *Vid*. «Proposal for a Regulation on Privacy and Electronic Communications», en *European Commission*, 10 January 2017. Disponible en Internet: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications [consulta: 02 de mayo de 2017]. Esta norma está íntimamente relacionada con el RGPD, respecto del cual constituye, de hecho, una norma especial, en el sentido de que sus disposiciones «*precisan y complementan*» las normas generales sobre la protección de los datos personales previstas en Reglamento (UE) 2016/679 «*estableciendo normas específicas*». PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), articulo 1 (Objeto). Sobre la propuesta de Reglamento, los expertos, incluido el profesor José Luis Piñar, han expresado dudas y problemas prácticos que la normativa trae consigo durante la jornada organizada en Madrid por Andersen Tax & Legal bajo el título "Futuro Reglamento europeo de e-Privacy: nuevas oportunidades de negocio". *Vid*. Carlos B. FERNÁNDEZ (2018), «El Reglamento de e-Privacy precisa y complementa al RGPD, pero plantea muchos problemas prácticos», en *Diario La Ley*, Wolters Kluwer, 31-1-2018.

[1539] *Cfr*. considerando 11 de la Directiva 95/46/CE: «*que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales*»; también el considerando 13 que «*las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario* (…)».

de privacidad. Por tal razón, se ha aprobado también la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que, como tendremos la oportunidad de aclarar, tiene sus límites en este sentido.

3.3. La transferencia internacional de datos personales a terceros países y el binomio privacidad-seguridad

120. La circulación de datos personales desde y hacia países fuera de la Unión y las organizaciones internacionales son necesarios para la cooperación internacional. El aumento de estos flujos ha planteado nuevos desafíos y preocupaciones con respecto a la protección de los datos personales, porque muy a menudo estos datos, individualmente o como resultado de sus agregaciones y combinaciones por parte de autoridades públicas, contiene información personal y, por lo tanto, se prestan a decir mucho sobre el carácter, costumbres, opiniones, actividades y experiencias de las personas, *etc*. Dado lo anterior, está claro que la transferencia de datos personales de la Unión Europea a terceros países no europeos es un tema particularmente relevante en el contexto económico, legal y político actual, por el hecho de que algunas de las disposiciones de la reforma han encontrado el consentimiento de los partidarios de "la necesidad de aumentar el nivel general de las medidas de seguridad pública, especialmente en lo que respecta a las normas que faciliten la transferencia de datos personales". Esto ha conllevado un aumento de los riesgos inherentes a que dicha información y datos personales sobre los individuos circulen sin la debida protección, al tiempo que se ha hecho más difícil el control de su uso y destino por parte del propio afectado.

121. Siendo así, merece una mención especial la cuestión de las transferencias de datos personales a terceros países, ya que constituye un desarrollo específico del conflicto normativo que ha dividido, y divide, por ejemplo, la UE y los Estados Unidos[1540] desde la

[1540] Conflicto que explotó en el período 2013-2015, tras las revelaciones de Edward Snowden sobre los programas de vigilancia masiva puestas en marcha por las agencias de inteligencia de EE.UU. *Vid*. Caspar BOWDEN (2013); Didier BIGO, Sergio CARRERA, Nicholas HERNANZ, *et ál*. (2013); Francesca BIGNAMI, Giorgio RESTA (2015), «Transatlantic Privacy Regulation: Conflict and Cooperation», en *Law and Contemporary Problems*, vol. 78, págs. 101-134. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705601 [documentos consultados: 06 de mayo de 2017].

entrada en vigor de la Directiva 95/46/CE[1541]. La transferencia de datos personales a terceros país ha sido particularmente importante con respecto a la cuestión del equilibrio entre la privacidad y la seguridad. En este ámbito, debe tenerse en cuenta la reiterada sentencia del TJUE en el asunto *Schrems*, que puede ser considerada, sin duda, uno de los más relevantes precedentes en el contexto de la reciente jurisprudencia europea en el debato sobre los derechos fundamentales y la seguridad.

122. En este ámbito también debe tenerse en cuenta el contenido del nuevo Acuerdo bilateral entre la Unión Europea y los EE.UU., el llamado "*Privacy Shield*", que ha provocado numerosas críticas, al igual que ocurrió con el precedente Acuerdo de "Puerto Seguro", y esto a pesar de las observaciones formuladas por el TJUE en el caso *Schrems*[1542] y de la aprobación de la nueva normativa sobre datos personales, por lo que implica necesariamente que "el nivel adecuado de protección" debe ser reconsiderado a la luz de la elevación del nivel de protección ofrecido por el nuevo texto normativo. Por lo tanto, no hay duda de que la transferencia de datos personales desde Europa a terceros países se encuentra, desde siempre, rodeada de garantías especiales, por el hecho de que implica, en la mayoría de las ocasiones, el paso de información de una zona con un alto grado de protección legal por el derecho a la intimidad hacia jurisdicciones en que el derecho a la vida privada no tiene las mismas garantías.

123. En general, la nueva normativa europea preserva las condiciones establecidas por la Directiva 95/46/CE[1543] con respecto a las transferencias internacionales de datos que quedan sometidas al cumplimiento de los principios de legitimidad de tratamiento. El concepto de "*adequacy*" (adecuación) sigue siendo fundamental en el RGPD, tal y como establecía la Directiva, como requisito esencial para permitir la transferencia a terceros países y

[1541] Encuentra su fundamento jurídico en el artículo 25, apartado 1, al afrontar la regulación de las transferencias de datos personales a un país tercero, más allá de las fronteras de la UE, que requiere, como nivel de protección para los interesados, que el «*país tercero de que se trate garantice un nivel de protección adecuado*». Por lo tanto, la "adecuación" del nivel de protección de datos existente en el tercer Estado es el requisito previo para la transferencia de datos fuera de la Unión Europea.

[1542] Consultar Capítulo IV *supra*.

[1543] La cuestión del acceso de las autoridades públicas de terceros países a los datos personales transferidos al exterior a través de los instrumentos previstos en los artículos 25 y 26 de la Directiva 95/46/CE y las medidas que deben adoptarse con el fin de garantizar el cumplimiento de los principios de necesidad y proporcionalidad, incluso si estos accesos se realizan sobre la base de las excepciones previstas por razones de justicia o la seguridad pública, ha sido foco de la actividad realizada por el Grupo de Trabajo a través de subgrupo *International Transfers*. En particular, el argumento ha sido tratado en el documento ARTICLE 29 DATA PROTECTION WORKING PARTY (2013d), Explanatory Document on the Processor Binding Corporate Rules, Adopted on 19 April 2013. As last revised and adopted on 22 May 2015, 00658/13/EN, WP 204 rev.01. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf [consulta: 07 de mayo de 2017].

organizaciones internacionales cuando "garantizan un nivel de protección adecuado", y la relativa decisión respecto a la evaluación del requisito de adecuación por la Comisión[1544].

124. La elección de la Unión en este sentido ha sido erigirse en un sólido modelo de protección de la privacidad, mediante la imposición a cualquier transferencia de datos personales de la UE para hacer frente al marco regulador europeo, garantizando a la información en tránsito un nivel de tutela particularmente elevada, modelada con precisión en el paradigma de la Directiva 95/46/CE. Conforme a este planteamiento, son tres las situaciones de transferencias de datos personales a terceros países u organizaciones internacionales reconocidas por el RGPD[1545], que se van a examinar: transferencias basadas en una decisión de adecuación (artículo 45); transferencias mediante garantías adecuadas (artículo 46); y normas corporativas vinculantes (artículo 47).

125. Como se ha indicado anteriormente, el RGPD tiende a extender su alcance más allá de las fronteras europeas en nombre de una protección real y efectiva para los interesados al exigir que todos los proveedores de servicios que promueven sus negocios también en los Estados europeos deben cumplir con el RGPD en el tratamiento de datos personales de los interesados europeos. Sin embargo, los Estados no pertenecientes a la UE no están sujetos al cumplimiento de las disposiciones del Reglamento y, como resultado, el nivel de seguridad, garantía y protección de los datos personales puede no coincidir con el establecido en las normas europeas.

126. Cuando los datos personales procedan de la Unión y se transfieran a los responsables, encargados u otros destinatarios en terceros países u organizaciones internacionales, el nivel de protección de esos datos garantizada en la UE por el RGPD no

[1544] Hasta ahora, la Comisión Europea ha reconocido que Andorra, Argentina, Canadá (organizaciones comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Suiza, Uruguay y EE.UU. (limitado al marco del "Escudo de la privacidad") brindan protección adecuada. *Vid*. «Adequacy of the protection of personal data in non-EU countries», en *European Commission*. Disponible en Internet: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en [consulta: 07 de mayo de 2017].

[1545] Capítulo V (Transferencias de datos personales a terceros países u organizaciones internacionales), artículos 44-50. *Vid*. artículo 44 (Principio general de las transferencias) del RGPD: «*Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado*».

puede verse comprometida, incluso en el caso de que se produjeran transferencias ulteriores del tercer país o de la «*organización internacional a responsables y encargados del tratamiento en el mismo u otro tercer país u otra organización internacional*». En efecto, «*las transferencias a terceros países y organizaciones internacionales solo pueden*» tener lugar si «*el responsable o encargado del tratamiento*» de datos «*cumple*» plenamente con «*las condiciones establecidas*» por las disposiciones del RGPD en relación con la transferencia de datos personales a terceros países u organizaciones internacionales (considerando 101).

127. Al igual que en la normativa precendenteel RGPD prevé una prohibición general de transferencia a terceros países u organismos internacionales[1546], pero admite que puedan realizarse «(…) *cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado*. *Dicha transferencia no requerirá ninguna autorización específica*»[1547]. Lo que se destaca es la ampliación de las entidades sometidas a evaluación por parte de la Comisión, en donde, además de los terceros países, las disposiciones sobre transferencias también toman en cuenta explícitamente las "organizaciones internacionales", así como "territorios y sectores". Es una novedad importante, que sin duda requerirá una mayor especificación a través de la interpretación,

[1546] El artículo 25 de la Directiva de 1995 estableció una prohibición general de la transferencia de datos personales fuera de la Unión Europea, aunque esta regla admitía una serie de excepciones. *Cfr*. Directiva 95/46/CE artículo 26 (Excepciones). *Cfr*. Davide BORELLI (2016), «La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali tra nuovo Regolamento europeo e (pre)vigente Direttiva», en *Diritto Mercato Tecnologia*, 10 Dicembre. Disponible en Internet: http://www.dimt.it/index.php/it/notizie/15688-la- [consulta: 08 de mayo de 2017]; Matteo LEFFI (2017b), «I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE», en *Rivista di Diritti Comparati*, núm. 1, October 27, págs. 187-205. Disponible en Internet: http://www.diritticomparati.it/wp-content/uploads/2017/11/Leffi8.pdf [consulta: 12 de noviembre de 2017].

[1547] Artículo 45 (Transferencias basadas en una decisión de adecuación), apartado 1, del RGPD. Será interesante ver las repercusiones que este artículo tendrá cuando haya sido traducido en hechos concretos el referéndum británico de 23 de junio del 2016 ("*Brexit*"), Gran Bretaña se encontrará sujeta al Capítulo V del Reglamento respecto a la transferencia de datos personales a terceros países. De acuerdo con el primer apartado del artículo 45, en ausencia de diferentes acuerdos, habrá una resolución de la Comisión que reconozca la adecuación del nivel de protección. Por otra parte, el Reglamento en vigor también en el Reino Unido, al igual que el resto de la legislación de la UE y permanecerá así hasta que se formaliza la salida de la UE. Cuando eso suceda, el destino del Reglamento 2016/679 dependerá del resultado de las negociaciones que tuvieron lugar, es decir lo que el nuevo Reino Unido fuera de la UE decidirá hacer de las directivas y reglamentos que se derivan de su pasado en varios campos de la Unión, incluyendo la protección de datos personales. Así que hay, incluso hoy en día, Estados europeos no comunitarios que tienen un sistema especial de integración con la UE, para lo cual el RGPD se aplica como si fueran miembros efectivos, sustrayéndolos al Capítulo V del Reglamento. Por lo tanto, pese a su anunciada salida de la Unión Europea, el gobierno británico adaptará al Reino Unido el contenido del RGPD con una nueva Ley de protección de datos ("*Data protection Bill*"), a fin de garantizar que el país se regirá en esta materia por los mismos principios que la Unión Europea, una vez se produzca el anunciado *Brexit* en marzo de 2019. Carlos B. FERNÁNDEZ (2017c), «El Reino Unido adapta su normativa sobre protección de datos al Reglamento europeo», en *Diario La Ley*, 21-8-2017.

pero que, en todo caso, permite una flexibilidad mayor que la anterior normativa. Además, sobre el concepto del nivel de protección "adecuado"[1548], la lectura del considerando 104 parece ser bastante clara: «*El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular,* (…) *debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas*»[1549].

128. En la elaboración de los elementos a considerar en la evaluación de la adecuación de la protección de datos el legislador europeo enuncia, por lo tanto, un alto nivel de detalle, con lo que se reduce la incertidumbre generada por la vaguedad parcial de ciertas disposiciones del artículo 25, apartado 2, de la Directiva de 1995[1550], y se deja espacio a la más completa y analítica norma contenida en el Reglamento, artículo 45, apartado 2. En particular, la Comisión al evaluar la adecuación del nivel de protección, tendrá en cuenta: «*a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos* (…)*, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización*

[1548] *Vid*. Davide BORELLI (2016) y Matteo LEFFI (2017b).

[1549] Debe tenerse en cuenta, además del considerando 104, también el considerando 105 y el 106 que detallan aún más los elementos que la Comisión debe tener en cuenta para evaluar la idoneidad requerida por el artículo 45, apartado 2, del RGPD (*infra*).

[1550] Efectivamente, la Directiva 95/46/CE no identifica un exhaustivo análisis y criterios para evaluar el "nivel adecuado de protección" ofrecido por la legislación de un tercer país; como tampoco el concepto de adecuación es objeto de una definición específica. Artículo 25 (Principios), apartado 2, de la Directiva 95/46/CE: «*El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*».

internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales»[1551].

129. El RGPD se diferencia de la Directiva de 1995, por un lado, ya que establece rigurosos requisitos de adecuación a través de la obligación de la Comisión para llevar a cabo una evaluación global que tenga en cuenta todo el marco regulatorio en el tercer país, restringiendo así su discreción para realizar dicha evaluación, tal como había sido solicitado por el TJUE en la sentencia *Schrems*[1552]; y, por otro, también de la protección contemplada en el caso de tratamientos con fines de policía y justicia y, en general, las protecciones existentes con respecto "el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales", "la seguridad pública", "la defensa", "la seguridad nacional y la legislación penal". La adopción de una decisión sobre adecuación debe «*tener en cuenta criterios claros y objetivos*», como las actividades de tratamiento específicas y «*el alcance de las normas jurídicas*» y «*legislación vigente en el tercer país*»[1553]. Además, en particular, debe tenerse en cuenta la adhesión del país al Convenio n. 108 y su Protocolo adicional.

[1551] La letra a) del artículo 45 del RGPD es más innovadora con respecto al artículo 25 de la Directiva 95/46/CE, ya que contiene un conjunto de requisitos impresionante y muy preciso que el tercero debe tener, con referencia a su legislación que podría decirse que tiene su propia visión política e ideológica del Estado de Derecho y de la democracia. *Vid*. Franco PIZZETTI (2016b: 162).

[1552] El concepto de "nivel de protección adecuado" al que nos referimos ha sido definido por el TJUE en el caso *Schrems*, en el que obliga al tercer país, de hecho, a garantizar, en virtud de «*su legislación interna o de sus compromisos internacionales, un nivel de protección de los derechos*» y libertades fundamentales que son esencialmente equivalentes a los protegidos dentro de la Unión Europea. El apartado 73 de la sentencia del TJUE asunto *Schrems* afirma: «*Es verdad que el término «adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo,* (…) *debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos*».

[1553] Considerando 104 del RGPD.

130. Debe tenerse en cuenta que en la sentencia *Schrems*, y ya antes en la sentencia *Digital Rights Ireland*, el TJUE también declaró que la discrecionalidad de la Comisión en cuanto a la adecuación del nivel de protección garantizado por un tercer país tenía que ser limitada, teniendo en cuenta, en primer lugar, el importante papel que desempeñan, como derechos fundamentales, la protección de los datos personales y el respeto de la vida privada y, en segundo lugar, el gran número de personas cuyos derechos fundamentales son susceptibles de ser vulnerados cuando los datos personales son transferidos a un tercer país sin garantizar un nivel adecuado de protección[1554]. En paralelo, la nueva normativa prevista por el RGPD promueve la cooperación con terceros países y organizaciones internacionales, sobre todo si la Comisión considera que garantizan, como se ha indicado, un "nivel de protección (de datos) adecuado", como prevé el artículo 45, apartado 3. En este sentido, el Reglamento manifiesta las exigencias del TJUE, también, bajo el aspecto obligatorio, a la Comisión «*tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional*»[1555], que podrían justificar modificaciones en la decisión de adecuación[1556].

131. En particular, si el tercer país «*ya no garantiza un nivel de protección adecuado*», inicialmente existente en la protección de los derechos de las personas que residen en la

[1554] TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 78: «*En ese sentido es preciso observar que, dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48)*».

[1555] Entre esta categoría de "acto de ejecución", se incluyen algunos acuerdos, tales como, por ejemplo, el "Puerto Seguro" o el nuevo "Escudo de la privacidad UE-EE.UU.".

[1556] *Cfr*. artículo 45, apartado 3, del RGPD: «(…) *El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2». Cfr*. artículo 45, apartado 4, del RGPD: «*La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE*».

Unión[1557], la Comisión tiene la obligación de derogar, modificar o suspender la decisión de adecuación, y también podrá adoptar una decisión de no idoneidad, mediante "actos de ejecución" *ex tunc*[1558]. Si la decisión es derogada, modificada o suspendida, por lo tanto, la Comisión, de conformidad con el apartado 6 del citado artículo, tiene el derecho a entrar en consultas con el tercer país u organización internacional para poner remedio a la situación[1559]. Por último, en relación con las decisiones adoptadas por la Comisión en aplicación de la Directiva 95/46/CE «*permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión* (…)»[1560].

132. Por lo tanto, parece que la Comisión es la institución de la Unión que tiene como un dominio indiscutido de las transferencias basado en una decisión de adecuación: una vez que tal decisión se adopte positivamente con referencia a un tercer país u organización internacional, la transferencia no necesitará más autorizaciones específicas por parte de los Estados. A este respecto cabe señalar que, si bien en el Reglamento se asigna un papel central a la Comisión, este mismo papel y función no se proporciona en la nueva Directiva (UE) 2016/680 (*vid*. más adelante). En fin, se presume que el objetivo de esta norma es, por lo tanto, evitar que los acuerdos de adecuación que se remontan en el tiempo mantengan sus efectos sin ningún control posterior por parte de la Comisión. El sistema global definido por el artículo 45, en relación con la evaluación de la adecuación de los terceros países, se basa en un sistema que parece dirigido por un "justo equilibrio" entre los intereses económicos, intereses públicos y los derechos fundamentales.

[1557] Artículo 45, apartado 5, del RGPD: «*Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2*».

[1558] Artículo 45, apartado 5, del RGPD.

[1559] «*La Comisión publicará en el Diario Oficial de la UE y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado*». Artículo 45, apartado 8, del RGPD.

[1560] Artículo 45, apartado 9, del RGPD. Esta característica también es válida para salvaguardar la efectividad del nuevo Acuerdo "Escudo de la privacidad UE-EE.UU." en la delicada transición de la validez de la Directiva 95/46/CE a la nueva regulación dictada por el Reglamento. Esto también se desprenderá del considerando 102 del Reglamento, donde se afirma que «*El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados*». *Vid*. Davide BORELLI (2016) y Matteo LEFFI (2017b).

133. En ausencia de una decisión de adecuación de la protección de los datos de la Comisión, la transferencia sólo será posible si el responsable o el encargado del tratamiento, han «*ofrecido garantías adecuadas*» y con la condición de que los interesados tienen derechos exigibles y remedios eficaces[1561]. Por lo tanto, se trata de una hipótesis alternativa a una decisión de adecuación del artículo 45. Según el artículo 46, apartado 2[1562], se regulan en detalle y de forma extensa tales "garantías adecuadas" para el interesado que pueden consistir en la aplicación de «*normas corporativas vinculantes*»[1563] (*Binding Corporate Rules - BCR*), a «*cláusulas tipo de protección de datos adoptadas por la Comisión*» o «*por una autoridad de control*», o «*cláusulas contractuales autorizadas por una autoridad de control*» ("*standard data protection clauses*"). Dichas garantías deben avalar el cumplimiento de los requisitos de protección de datos y los derechos de las personas interesadas en relación con el tratamiento dentro de la Unión, incluida la disponibilidad de los derechos exigibles de las personas afectadas y recursos efectivos, incluido «*el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización en la Unión o en un tercer país*». Deberían cubrir, en particular, el «*cumplimiento de los principios generales relativos al tratamiento de datos personales y los principios de protección de datos desde el diseño y por defecto*» (considerando 108). Las autoridades públicas u organismos públicos pueden realizar transferencias a autoridades públicas u organismos públicos de terceros países u organizaciones internacionales con competencias o funciones similares, incluso sobre la base de disposiciones que deben incluirse en «*acuerdos administrativos como un memorando de entendimiento*» que prevea los derechos efectivos y viables de los interesados. La «*autorización de la autoridad de control competente*» debería obtenerse cuando las garantías se ofrezcan en virtud de acuerdos administrativos no jurídicamente vinculantes (considerando 108).

[1561] *Vid*. artículo 46 (Transferencias mediante garantías adecuadas), apartado 1, del RGPD: «*A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas*».

[1562] Artículo 46, apartado 2, del RGPD: «*Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por: a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión* (…)*; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión* (…)*; e) un código de conducta* (…)*, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación* (…)*, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados*».

[1563] Sobre las normas corporativas vinculantes el Reglamento dedica, concretamente, el artículo 47 (Normas corporativas vinculantes). Para un mayor desarrollo del alcance de las normas en comento, *vid*. *supra* el apartado relativo a la sentencia *Schrems* e *infra*.

134. Con respecto a las "garantías adecuadas" que requieren la autorización de la autoridad de control competente, de conformidad con el "mecanismo de coherencia", se hace referencia a dos hipótesis: «*a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados*» (artículo 46, apartado 3)[1564].

135. De una comparación con el artículo 26 de la Directiva 95/46/CE – que hacía mención únicamente a las cláusulas contractuales tipo –, se desprende que la nueva reglamentación ha ampliado considerablemente la gama de instrumentos en los que puede basarse la transferencia internacional de datos. En algunos casos se trata de mecanismos ya ampliamente difundidos en la práctica, que sin embargo se beneficiarán de la provisión de una base legal clara en el RGPD. En otras palabras, el hecho de que el legislador europeo se haya preocupado por dictar una normativa específica debería dificultar la elusión de los principios de protección de datos personales y evitar abusos que afecten a los interesados[1565].

136. El siguiente artículo 47, que se dedica totalmente a las normas corporativas vinculantes[1566], da testimonio de la importancia y papel de este instrumento en el sistema

[1564] Artículo 46, apartado 4, del RGPD. El mecanismo de coherencia, introducido por el artículo 63, es un sistema «*A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia* (…)». «*Este mecanismo debe aplicarse en particular en el momento en que una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten a un significativo número de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe comprenderse sin perjuicio de medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados*». Considerando 135 del RGPD. A este respecto cabe señalar que, si bien en el RGPD el legislador de la UE asigna un papel central a la Comisión en el mecanismo de coherencia, no se proporciona tal función en la nueva Directiva de protección de datos en el sector policial y judicial, *vid*. *infra*.

[1565] EDPS (2012: 35).

[1566] Las normas corporativas vinculantes son instrumentos utilizados por un «*grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta*» para la transferencia de datos personales de un País de la UE a «*organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal*». Constituyen una especie de código de conducta interno para las empresas multinacionales, que establece una política de privacidad colectiva a nivel mundial y regula las transferencias a todas las sucursales de la empresa, independientemente de su ubicación. No se pueden utilizar las normas corporativas vinculantes, por lo tanto, cuando la entidad que recibe los datos personales no se refiere al grupo de sociedades. *Cfr*. considerando 110 del RGPD. Sobre las normas o reglas corporativas vinculantes, interesante son los contributos de Alfonso ORTEGA GIMÉNEZ (2015: 47-50) y de Miguel RECIO GAYO (2017b), «Normas Corporativas Vinculantes (BCRs): comentarios a los nuevos documentos de trabajo del GT29», en *Diario La Ley*, Sección Ciberderecho, núm. 1, 12 de diciembre.

europeo de transferencia de datos personales a terceros países. En este sentido, se prevé que la autoridad de control competente apruebe las «*normas corporativas vinculantes*» de acuerdo con el "mecanismo de coherencia", siempre que estas: «*a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados; b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y c) cumplan los requisitos establecidos en el apartado 2*». Este apartado 2 enumera una larga lista de información que las normas corporativas vinculantes deben especificar necesariamente (*condicio sine qua non*): a) «*la estructura y los datos de contacto del grupo empresarial*» o grupo de empresas y de cada uno de sus miembros; b) «*las transferencias o el conjunto de transferencias de datos*»; c) su naturaleza jurídicamente vinculante, tanto a nivel interno como externo; d) «*la aplicación de los principios generales de protección de datos*»[1567]; e) los derechos de la persona interesada «*en relación con el tratamiento y los medios para ejercerlos*», incluyendo el derecho a no ser sometido a «*decisiones basadas*» únicamente «*en un tratamiento automatizado*», incluyendo la elaboración de perfiles[1568], «*el derecho a presentar una reclamación*» a la «*autoridad del control competente y ante los tribunales competentes de los Estados*» miembros[1569], y «*el derecho a obtener reparación*» y, en su caso, «*una indemnización*» por incumplimiento de normas corporativas vinculantes; f) el hecho de que el responsable del tratamiento o encargado establecidos en el territorio de un Estado miembro sea responsable «*de cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión*»; g) las modalidades en las que se proporcionan la información sobre las normas corporativas vinculantes[1570]; h) «*las funciones de todo delegado de protección de datos designado*»; i) «*los procedimientos de reclamación*»; j) «*mecanismos dentro del grupo empresarial o grupo*

[1567] En particular con respecto a «*la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes*».
[1568] *Vid. supra*.
[1569] Artículo 79 (Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento) del RGPD: «*1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control* (…)*, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales. 2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos*».
[1570] Disposiciones contempladas en los artículos 13 y 14 del RGPD.

de empresas para garantizar el cumplimiento de las normas corporativas vinculantes»; k) mecanismos para comunicar y registrar los cambios en las normas y notificarlos a la autoridad de control; l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento de las normas corporativas vinculantes; m) «*los mecanismos para informar a la autoridad de supervisión competente*» de todos los requisitos legales que se aplican en un tercer país que podrían tener «*un efecto adverso*» significativo «*sobre las garantías*» previstas por el normas corporativas vinculantes; y n) formación adecuada en «*protección de datos para el personal*» que tiene «*acceso permanente*» o regular a datos personales.

137. Por lo que respecta a las «*transferencias o comunicaciones no autorizadas por el Derecho de la Unión*», el Parlamento Europeo promovió la introducción del artículo 48 RGPD que responde al escándalo de la *NSA*, y que prevé la mediación institucional de las autoridades europeas de protección de datos en los casos de tratamientos de datos a efectos judiciales por las autoridades extranjeras ("*anti-PRISM privacy clause*")[1571]. En este sentido, prohíbe las transferencias solicitadas por las autoridades judiciales o administrativas de terceros países cuando no encuentren fundamento en los acuerdos internacionales sobre asistencia mutua jurídica o instrumentos similares, bilateral o multilateral: «*Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo*». Está claro que la intención del legislador europeo es evitar que las transferencias internacionales permitan a las autoridades públicas de terceros países el acceso a los datos sin las garantías adecuadas, requisito subrayado por el Grupo de Trabajo[1572], que ha propuesto una interpretación restrictiva de esta parte del Reglamento.

[1571] Peter BRADWELL (2013), «EU Commission caved to US demands to drop anti-PRISM privacy clause», en *Open Rights Group*, June 14. Disponible en Internet: https://www.openrightsgroup.org/blog/2013/how-the-eu-commission-caved-to-us-demands-to-water-down-its-privacy-law; «PRISM Scandal - EPP Group to push introduction of 'Anti-net tapping clause'», en *EPP Group*, 19.06.2013. Disponible en Internet: http://www.eppgroup.eu/press-release/PRISM%3A-we-want-introduction-of-'Anti-net-tapping-clause' [documentos consultados: 19 de mayo de 2017].

[1572] ARTICLE 29 DATA PROTECTION WORKING PARTY (2015d), Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Adopted on 22 September 2015, 2588/15/EN, WP 232, págs. 7 y ss. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf [consulta: 19 de mayo de 2017].

138. Con especto a las tres situaciones que se han mencionado anteriormente – es decir "transferencias basadas en una decisión de adecuación", "transferencias mediante garantías adecuadas" y "normas corporativas vinculantes" – existen excepciones específicas previstas por el legislador europeo que legitiman la transferencia de datos en circunstancias en que no se garantice el nivel adecuado de protección requerido por el Reglamento[1573], y que no introduce ninguna innovación particular con respecto a la Directiva de 1995. En particular, la transferencia de datos personales a un tercer país u organización internacional únicamente es admisible sólo si se cumple alguna de las ocho condiciones siguientes[1574]: «*a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas; b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado; c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; d) la transferencia sea necesaria por razones importantes de interés público; e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones; f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo* (…)»[1575].

139. Si se hace una comparación con el artículo 26 de la Directiva de 1995, existe una correspondencia sustancial con la legislación anterior, sin perjuicio de la disposición de requisitos más estrictos para la validez del consentimiento. Continuando con la lectura del apartado 2 del artículo 49, parte segunda, encontramos un elemento de novedad real que no se encuentra en la norma previa. En otras palabras, la transferencia a países no pertenecientes a la UE sólo «*se podrá llevar a cabo si no es repetitiva*», se refiere a un número limitado de personas interesadas y «*es necesaria a los fines de intereses legítimos imperiosos*

[1573] Artículo 49 (Excepciones para situaciones específicas), apartado 1, del RGPD.
[1574] Las excepciones a una prohibición general de la transferencia de datos personales a países terceros que no garanticen un nivel adecuado de protección, previstas por el artículo 49 del RGPD, son sustancialmente las mismas que establecía el artículo 26 de la Directiva 95/46/CE.
[1575] *Cfr*. considerando 112 del RGPD.

perseguidos por el responsable del tratamiento», sobre los que no prevalecen «*los intereses, derechos y libertades del interesado*», y si el responsable del tratamiento ha evaluado «*todas las circunstancias concurrentes en la transferencia*» y sobre la base de esa evaluación ha proporcionado «*garantías adecuadas con respecto a la protección de los datos*» personales[1576]. En tales ocasiones, el responsable del tratamiento informa a la autoridad de control y, además de la información estándar habitual[1577], informa a la persona interesada sobre la transferencia y los intereses legítimos imperiosos perseguidos[1578].

140. Fuera de estas situaciones "ordinarias" y "excepcionales", nunca se permite la transferencia de datos personales a terceros países u organizaciones internacionales.

141. Por último, otra novedad importante figura en el artículo 50 (Cooperación internacional para la protección de datos personales). Tanto la Comisión como las autoridades nacionales de control[1579], en relación con los terceros países y las organizaciones

[1576] El responsable del tratamiento «*debe prestar especial atención a la naturaleza de los datos personales, finalidad y la duración*» del tratamiento o tratamientos propuestos, «*así como la situación en el país de origen*», «*en el tercer país*» y en «*el país de destino final*», y debe ofrecer garantías adecuadas para la protección de los derechos y libertades fundamentales de las personas físicas con respecto al tratamiento de sus datos personales.
[1577] Según los artículos 13 y 14 del RGPD.
[1578] Artículo 49, apartado 1, segunda parte. Esta hipótesis despierta algunas perplejidades, porque aparece formulada en términos extremadamente genéricos. En primer lugar, con respecto al significado del término "repetitivo", no está claro si debe ser una transferencia única o si existe una posibilidad limitada de repetirla. En segundo lugar, incluso la referencia al número limitado de persona interesadas es vaga: ¿cuál es el punto de referencia para apreciar el número limitado de personas interesadas? ¿Deberíamos referirnos al tamaño de la población del Estado o más bien en ámbito europeo? De todos modos, la hipótesis en cuestión es residual y está destinada a operar cuando ninguna de las otras condiciones para la transferencia de datos personales en el extranjero es aplicable (cuando una transferencia no pueda basarse en las disposiciones de los artículos 45 o 46).
[1579] La importancia del control que se puede definir "técnico" por parte las autoridades de control junto con un control parlamentario y judicial, que puede entonces ser combinado con un "tríptico" de parámetros tales como aquel político, de legitimidad jurídica y de proporcionalidad en términos de privacidad, todas medidas necesarias para prevenir una recopilación excesiva, lo que haría degenerar un control estratégico en la vigilancia masiva. En este sentido, entonces, las competencias, funciones y poderes también en materia de acceso a bases de datos, reconocidos a las autoridades, representan esencialmente una garantía con respecto al acceso ilegal por parte de terceros, pero no permiten evitar las adquisiciones de datos, hechas formalmente por sujetos legitimados, que sean, en realidad, no justificados por motivos reales de protección de la seguridad nacional. Pues, la función de garantía de la autoridad debe tener en cuenta esta evolución y debe, por lo tanto, llevarse a cabo de acuerdo con las formas más adherentes a las mismas actividades objeto de análisis, centrándose más específicamente en la seguridad y los sistemas de datos con la que los diferentes tratamientos se llevaron a cabo que no, en cambio, sólo a la legalidad de cada tratamiento. Esta función de garantía de las autoridades de control es ampliamente reconocida en los ordenamientos jurídicos europeos, de la que el RGPD es un ejemplo obvio, especialmente en el actual contexto histórico en el que la progresiva expansión de los poderes informativos de los servicios de inteligencia, parecen no interesase el valor que tiene el respeto de la misma vida privada. De la importancia que revisten las autoridades nacionales de control y en relación con el nuevo Reglamento, interesante es el artículo de Noemí BRITO y Francisco Javier CARBAYO (2016), «Autoridades europeas de protección de datos: clave de salvaguarda de la privacidad», en *Red Seguridad*, 14/01/2016. Disponible en Internet: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/autoridades-europeas-de-proteccion-de-datos-clave-de-salvaguarda-de-la-privacidad [consulta: 21 de mayo de 2017].

internacionales, tendrán que desarrollar «*medidas apropiadas*» para crear mecanismos de cooperación internacional «*a) que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales; b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales; c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales; d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países*». Esto constituye un desarrollo innovador, especialmente en lo que respecta a la participación directa en las relaciones internacionales por parte de los órganos internos, que son las autoridades nacionales de control.

142. En conclusión, se puede deducir que, por lo tanto, todo el sistema de la transferencias de datos personales a terceros países u organizaciones internacionales basado en la Directiva de 1995 parece haber fracasado en uno u otro de sus objetivos[1580], como es la protección de las personas con respecto al tratamiento de los datos personales y el fortalecimiento de la libertad de movimiento de los datos como instrumento para promover la competitividad de las empresas europeas en el mercado interior y en el comercio internacional. Frente a esto, sin embargo, el nuevo RGPD no introduce cambios sustanciales en la normativa sobre transferencia de datos a terceros países. El principio general es siempre la autorización condicionada, con la decisión de adecuación de la Comisión sobre el nivel de protección adecuado por el tercer Estado, o por la decisión de no adecuación; todavía están permitidos los instrumentos jurídicos vinculantes para la transferencia de datos a terceros países que no garanticen un nivel adecuado de protección; y sigue existiendo la posibilidad de transferencias con excepciones para situaciones específicas.

[1580] *Cfr*. considerando 9 del RGPD.

4. La Directiva de protección de datos para asuntos policiales y judiciales: En busca de un equilibrio entre seguridad y protección de derechos fundamentales

143. Cuando la Comisión Europea publicó sus propuestas de reforma integral de las normas de protección de datos de la UE en enero de 2012, los profesionales de la privacidad y los comentaristas centraron su atención casi exclusivamente en el proyecto de RGPD[1581]. Desde entonces, las negociaciones sobre una directiva complementaria de protección de datos se han llevado a cabo de forma paralela a la del RGPD pasando casi inadvertida. Sin embargo, los graves ataques terroristas y, en particular, el de París, realzaron la importancia de la directiva relativa al tratamiento de datos personales en asuntos policiales. En efecto, el contexto histórico es determinante porque los ataques terroristas reactivaron una discusión de larga duración sobre la tensión entre mantener la seguridad pública y al mismo tiempo garantizar que se respeten los derechos de protección de datos de las personas[1582].

144. Tras la entrada en vigor del Tratado de Lisboa, que permitió la adopción de un único instrumento de protección de datos, surgió la oportunidad de remediar las críticas a la Decisión Marco 2008/977/JAI y, al mismo tiempo, de construir un único sistema coherente de protección de datos personales en la Unión Europea[1583]. Sin embargo, la opción del legislador europeo por un reglamento como instrumento de protección de datos general en

[1581] Joseph A. CANNATACI (2013), «Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector», en *European Journal of Law and Technology*, vol. 4, núm. 2, págs. 35.

[1582] La criminalidad y los fenómenos como el terrorismo, tanto en la organización como en la estructura y *modus operandi*, han evolucionado. De hecho, el crimen internacional, así como el terrorismo islámico, hacen uso constante de la tecnología, por ejemplo, para la propaganda o educación de los adeptos, o usan directamente la herramienta de Internet para perpetrar los delitos en sí (piense en el delito cibernético). También se observa la constante actualización y evolución del factor tecnológico. De hecho, el proceso tecnológico y de globalización ha cambiado significativamente la recopilación, consulta, uso, almacenamiento y transferencia de datos personales.

[1583] Artemi RALLO LOMBARTE (2012), «Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma», en *UNED. Revista de Derecho Político*, núm. 85, septiembre-diciembre, págs. 32 y ss. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/10244 [consulta: 23 de mayo de 2017]. La Comunicación de la Comisión de 2003, que revisó el estado de implementación de la Directiva 95/46/CE por primera vez, indicó que no era necesario realizar cambios legislativos. La situación necesitaba mejoras y el informe de la Comisión contenía un programa de trabajo para una mejor implementación de la Directiva de 1995. En 2007, la Comisión emitió una nueva comunicación y aun así no consideró necesario enmendar la Directiva. Esto fue antes de la firma del Tratado de Lisboa en 2007, después de la cual cambió la opinión de la Comisión. En 2009, la Comisión publicó una nueva consulta con una sección sobre la protección de los datos personales y la privacidad, donde sostenía que la UE tenía que responder al desafío planteado por el creciente intercambio de datos personales y la necesidad de proteger la privacidad. La Comisión hizo referencia a los derechos de la CDFUE, y sugirió que las iniciativas legislativas pueden ser necesarias. *Vid*. INFORME DE LA COMISIÓN - PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46 CE) (2003); COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos (2007); COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL (2009).

la UE, hizo extremadamente difícil intervenir en este ámbito. De hecho, el tema sigue siendo delicado: las actividades de tratamiento de datos policiales fueron, hasta hoy, regulados por la Decisión Marco del Consejo de 2008 mientras que el Reino Unido, Irlanda y Dinamarca pueden optar por salir de los instrumentos adoptados en el ámbito del ELSJ (Protocolos núms. 21, 22 y 36)[1584]. La elección del instrumento legislativo de una directiva, sin embargo, dejaba un amplio margen de apreciación a los Estados miembros que podría poner en peligro el objetivo de armonización de ésta.

145. Tras una tramitación casi olvidada y marginada por los medios de comunicación, el 4 mayo de 2016 fue publicada, en el mismo número del Diario Oficial de la Unión Europea que publicó el nuevo RGPD[1585], la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[1586]. La estructura de la Directiva está sustancialmente alineada al RGPD que mantiene, sin cambios, la articulación en Capítulos[1587] y la correspondencia de los títulos.

[1584] Protocolo (n. 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia; Protocolo (n. 22) sobre la posición de Dinamarca; Protocolo (n. 36) sobre las disposiciones transitorias. En VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA.

[1585] La nueva Directiva, como sabemos, forma parte de la modernización de los instrumentos jurídicos relativos a la protección de los datos personales que ha llevado a la conclusión de un largo proceso legislativo europeo de la protección de datos europeo, que se compone, además del citado RGPD que regula el tratamiento de datos personales tanto en el sector público y privado destinado a sustituir a la Directiva 95/46/CE; de la Directiva dirigida a la regulación de ámbitos de prevención, lucha y represión de los crímenes, y para la ejecución de las penas, que sustituirá e integrará la Decisión Marco 2008/977/JAI. *Vid*. Cristina BLASI CASAGRAN (2016b); Thomas MARQUENIE (2017), «The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework», en *Computer Law & Security Review*, vol. 33, issue 3, June, págs. 324-340; Lauri J. PAJUNOJA (2017), *The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU's data protection law and its compatibility with the right to privacy*, Master's thesis, University of Helsinki Faculty of law, The Erik Castrén Institute of International Law and Human Rights Public international law, págs. 96; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018: 271-291).

[1586] Artículo 59 (Derogación de la Decisión Marco 2008/977/JAI) de la Directiva (UE) 2016/680. Este es un reemplazo que ningún defensor de la protección de datos lamentará. Así en Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016: 8). El derecho al respeto de la vida privada y familiar se menciona en la Directiva como uno de los derechos de la Carta que en particular merecen respeto. La palabra "privacidad" no está en el texto final, pero la Directiva pretende respetar los derechos fundamentales de «*la Carta, consagrados en el TFUE, en particular el derecho al respeto de la vida privada y familiar, el derecho a la protección de los datos personales y el derecho a la tutela judicial efectiva y a un juez imparcial*». Considerando 104 de la DIRECTIVA (UE) 2016/680.

[1587] El texto de la Directiva se compone de X Capítulos, 65 artículos y 107 considerandos. Los primeros cinco capítulos describen "el alcance de la Directiva", "los principios generales relativos al tratamiento de los datos personales", "los derechos del interesado", "las obligaciones del responsable del tratamiento y encargado del tratamiento", "las medidas técnicas y de organización necesarias para garantizar la seguridad de los datos

146. El objetivo de la Directiva es ampliar el nivel de protección de datos atribuido a las personas y abordar las deficiencias y las excesivas limitaciones de la Decisión Marco de 2008. La Directiva, a diferencia de la Decisión Marco, confiere efecto directo a los individuos, se somete a la CDFUE, cuenta con la participación del Parlamento Europeo en el procedimiento legislativo y entra en el campo de jurisdicción del TJUE[1588]. En particular, la Decisión Marco sólo se aplicaba al tratamiento de datos transfronterizos, ni siquiera a las actividades de la policía que se llevan a cabo a nivel nacional[1589]. La consecuencia inmediata ligada a esta restricción fueron unas grandes dificultades que encontraron las fuerzas del orden y otras autoridades competentes en los ámbitos de la cooperación judicial en materia penal y policíal, ya que, como se indica en la Comunicación de la Comisión: «*no siempre está claro si el tratamiento de datos ha de ser exclusivamente nacional o internacional, o si los datos nacionales pueden ser objeto de un intercambio internacional subsiguiente*»[1590]. Por lo que, en ausencia de un marco armonizado de los principios de protección de datos en este sector específico debido a la incompleta integración desarrollada en este sentido[1591], se dictó la nueva norma sobre la protección de datos personales tratados en el marco de la cooperación judicial en materia penal y de la cooperación policial.

147. Desde su aprobación, la Directiva (UE) 2016/680 ha sido presentada como clave para mejorar la cooperación en toda Europa "con el fin de garantizar un elevado nivel de protección de datos al tiempo que mejora la cooperación en la lucha contra el terrorismo y otros delitos graves"[1592]. La Directiva nace para facilitar el intercambio de datos mediante

personales", "las cuales tendrán que ser adoptadas por ellos", y, por último, "la regulación de la transferencia de datos personales a terceros países u organizaciones internacionales". La segunda parte de la Directiva regula "el estatus, funciones y competencias de las autoridades de control independientes" y establece "el derecho a presentar reclamación ante una autoridad de control", "el derecho a un recurso judicial" y "el derecho a una indemnización por cualquier persona que haya sufrido daños materiales o inmateriales" como consecuencia de un tratamiento ilícito de datos personales.

[1588] Así, cualquier juez nacional puede referir una cuestión prejudicial sobre datos tratados con fines policiales al TJUE. Steve PEERS (2012), «Analysis. The Directive on data protection and law enforcement: A Missed Opportunity?», en *Statewatch*, April, págs. 5. Disponible en Internet: http://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf [consulta: 25 de mayo de 2017].

[1589] Véase Capítulo II, *supra*.

[1590] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, COM/2012/09 final.

[1591] Durante nuestra investigación, a menudo se ha recalcado en varias ocasiones que el marco normativo general a nivel europeo sobre cooperación judicial y policial ha resultado incompleto y fragmentado, una fuente de malentendidos inevitables tanto en términos de interpretación como en términos de aplicación, entre los Estados miembros. Una intervención regulatoria en este sector, capaz de llevar la disciplina de nuevo a un camino de equilibrio aceptable entre privacidad y seguridad pública, ha sido invocada repetidamente, especialmente debido a la evolución de los elementos fundamentales de la ecuación de cooperación entre la justicia y la policía.

[1592] En particular: «*These new rules come at a time when improved cooperation across Europe in the fight against terrorism and other serious crime is of utmost importance. The new directive will allow for smoother cooperation and exchange of information between member states' police and judicial authorities based on a*

una norma común de protección de datos y para proteger a los ciudadanos de la UE contra la vigilancia masiva o la recogida indiscriminada de datos[1593]. La Directiva también se aprueba después de las sentencias *Digital Rights Ireland* y *Schrems*, en las que el TJUE fijó criterios importantes para el respeto de los derechos fundamentales a la intimidad y la protección de datos en el ámbito de aplicación de la ley, dando pautas concretas para los "*policy makers*" de la UE sobre cómo garantizar el pleno cumplimiento de los derechos fundamentales en las políticas de seguridad de la UE[1594].

148. La Directiva (UE) 2016/680, permite a los Estados miembros un cierto "nivel de flexibilidad" en sus respectivas legislaciones nacionales, mientras que el RGPD regula el tratamiento general de los datos personales. De este modo, la UE reconoció un proceso a dos velocidades en el esfuerzo por armonizar todo el proceso de los datos personales de la UE[1595]: el nivel de protección reconocido en la Directiva para la protección de datos en los sectores de la policía y la justicia es mucho menor de lo establecido en el RGPD. Concretamente, como se ha indicado anteriormente[1596], el hecho de que la propuesta no haya sido adoptada en forma de reglamento ha suscitado críticas entre varios sectores defensores de la protección de datos en la UE, que han expresado su descontento y han puesto de

common standard of data protection. And the rules will ensure that personal data, for instance of victims or witnesses of crime, is properly protected and that no mass surveillance or indiscriminate bulk collection of citizens' data is allowed». Así han declarado Jan Philipp ALBRECHT, Marju LAURISTIN and Věra JOUROVÁ (2016), «New data protection rules fit for our digital age», en *Fondation EURACTIV*, 14 apr. Disponible en Internet: http://www.euractiv.com/section/digital/opinion/new-data-protection-rules-fit-for-our-digital-age/ [consulta: 25 de mayo de 2017].

[1593] Mediante sentencia del 6 de febrero de 2015 el *Investigatory Powers Tribunal* –la corte a la que, en el Reino Unido, se remitían las controversias sobre la aplicación de *Regulation on Investigatory Power Act 2000* ("*RIPA*")– estableció que la vigilancia masiva y transmisión de datos (información confidencial distribuido por correo electrónico entre las ONG estadounidenses y británicos), actuada por las autoridades británicas bajo el programa *PRISM* y *Upstream* de EE.UU., era contraria a los artículos 8 y 10 del CEDH. El fallo parece sugerir que los aspectos de las operaciones fueron ilegales durante al menos siete años, entre 2007, cuando se introdujo el programa de interceptación PRISM, y 2014. *Amplius*, Owen BOWCOTT (2015), «UK-US surveillance regime was unlawful 'for seven years'», en *The Guardian*, Fri 6 Feb 2015. Disponible en Internet: https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa [consulta: 26 de mayo de 2017].

[1594] Precisamente en relación con estos aspectos, mientras que el Consejo de la UE aprobaba la discusión del proyecto ("*general approach*") con el Parlamento Europeo, el TJUE pronunciaba la sentencia *Schrems*. De hecho, el 6 de octubre de 2015 el TJUE declaró "la nulidad de la decisión de la Comisión Europea", según la cual los EE.UU. "no tenían un nivel adecuado de protección de datos personales". El tema planteado es complejo, pero indicativo de los problemas que se entrelazan en el campo del procesamiento transfronterizo de datos personales. Como se indicaba anteriormente en la parte relacionada al RGPD, la pasada Directiva 95/46/CE establecía que el tratamiento de dichos datos a un tercer país sólo podrá tener lugar si se garantiza un nivel adecuado de protección. La Comisión puede determinar que un tercer país, en vista de su legislación nacional o de sus compromisos internacionales, garantiza un nivel adecuado de protección. Sin embargo, la decisión de la Comisión no tiene fuerza vinculante en términos absolutos: en particular, no se opone a que las autoridades públicas designadas en cada Estado miembro puedan comprobar las condiciones de protección de datos en el tercer Estado. Este principio, se mantiene en la nueva Directiva (UE) 2016/680.

[1595] Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016: 9).

[1596] *Cfr*. *supra* EDPS (2012); ARTICLE 29 DATA PROTECTION WORKING PARTY (2013a).

manifiesto que el nivel de protección de datos que ofrece la propuesta de Directiva es inadecuado, ya que es muy inferior al de la propuesta para un RGPD. De tal manera, si los derechos previstos en el RGPD se ejercieran en la mayor medida posible dentro de los fines reconocidos en la Directiva de protección de datos para asuntos policiales y judiciales[1597], sería efectivamente casi imposible realizar investigaciones criminales[1598]. Es por ello por lo que las necesidades especiales relacionadas con la seguridad tienen que ser reconocidas en el texto de la Directiva de protección de datos en sectores de policía y justicia.

149. La Directiva (UE) 2016/680 tiene como base jurídica específica la afirmación del derecho fundamental a la protección de datos contenida en el artículo 16 del TFUE, realizada por la Comisión para ambos instrumentos de la reforma. Con la nueva Directiva se da realización al mando proporcionado por el mismo artículo 16 del TFUE, que obliga el Parlamento Europeo y el Consejo a establecer normas relativas a la «*protección de las personas físicas respecto del tratamiento de los datos de carácter personal y sobre la libre circulación de estos datos*», incluida la cooperación judicial en materia penal y la cooperación policial[1599]. Sin embargo, debido a la naturaleza específica del alcance de la cooperación policial y judicial en materia penal, se reconoció claramente en la Declaración n. 21, relativa a la protección de datos de carácter personal en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial, adjunta al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, la necesidad de normas específicas para la cooperación penal y policial[1600]. Se consigue así que, de acuerdo con el enfoque de las instituciones europeas, el tratamiento en contexto de policía y justicia penal se diferencia de todos los demás tratamientos de datos personales[1601].

[1597] *Vid*. *infra*.
[1598] Por ejemplo, los principios de minimización de datos y limitación de objetivos, que exigen que los datos personales se limiten sólo a lo necesario en relación con los fines para los que se tratan, y que se procesen para fines específicos y explícitos, también deben aplicarse de forma flexible al procesamiento relacionado con la seguridad. La información recopilada y almacenada por las autoridades competentes para un caso particular puede resultar extremadamente útil para resolver casos futuros.
[1599] Considernado 8 y 10 de la DIRECTIVA (UE) 2016/680.
[1600] En la Declaración n. 21, relativa a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, aneja al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa, «*la Conferencia reconoce que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en razón de la naturaleza específica de dichos ámbitos*». La Declaración n. 21 reconoce que la naturaleza específica del campo de seguridad merece un tratamiento legislativo especial. *Vid*. considerando 10 de la DIRECTIVA (UE) 2016/680; también véase Cristina BLASI CASAGRAN (2015: 137).
[1601] Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016: 8).

150. Tal y como se ha analizado anteriormente, la Directiva apunta a equilibrar los objetivos de protección de datos con los objetivos de política de seguridad y, aunque sin duda contribuye a la creación de un marco general menos fragmentado, no resuelve todas las deficiencias que habían surgido antes de su adopción. Ese problema se presenta desde el principio debido a la arquitectura del paquete de reformas sobre la protección de datos: la creación de un Reglamento y una Directiva. La opción elegida, representa una posición intermedia: por un lado, extiende el marco de aplicación de la Directiva al trato nacional o doméstico y otras críticas mencionadas a la Decisión Marco; por el otro, no resuelve el problema de establecer criterios comunes dentro los Estados en el tratamiento de datos personales por razones de prevención y represión penal de todos los operadores jurídicos. Tanto la Decisión Marco 2008/977/JAI como la Directiva de protección de datos para asuntos policiales y judiciales excluyen muchos de los instrumentos de derecho derivado que ha ido adoptando la UE para permitir el intercambio de datos personales. La razón de tal exclusión es principalmente política, ya que muchos Estados miembros consideraron que centralizando las normas de protección de datos en un único acto legislativo perderían sus competencias en la regulación de medidas en el ámbito de la seguridad interior[1602]. Por lo tanto, tanto la Decisión Marco como la nueva Directiva incluyen una cláusula que prevé que las normas anteriores sobre protección de datos prevalecerán a estos actos legislativos[1603]. Así que, el valor añadido real de la Directiva (UE) 2016/680 dependerá mucho de su aplicación en la legislación nacional y de los tribunales nacionales[1604], así como del TJUE, con el fin de garantizar que la Directiva de protección de datos en los sectores policial y judicial contribuye a una mejor protección de datos en la UE.

[1602] Cristina BLASI CASAGRAN (2015: 141).

[1603] *Cfr*. artículo 28 (Relación con actos de la Unión adoptados previamente) de la DECISIÓN MARCO 2008/977/JAI y artículo 60 (Actos jurídicos de la Unión en vigor) de la DIRECTIVA (UE) 2016/680.

[1604] El SEPD, además de comentar sobre la propuesta de RGPD, comentó la propuesta de la Directiva de protección de datos en materia policial. Estableció que la protección de datos está estrechamente relacionada con el valor fundamental del derecho a la privacidad. La propuesta de la Directiva respeta las obligaciones legales establecidas en la legislación internacional y de la UE, y reconoce que la privacidad y la protección de datos son valores fundamentales para la sociedad y sus individuos. El SEPD afirmó que se necesitan normas específicas debido a la naturaleza específica de los sectores de policía y justicia. La protección de datos en estos sectores debe ser coherente con las reglas generales escritas en el RGPD y especificarse sólo si es necesario. Según el SEPD, el Consejo modificó la naturaleza de la Directiva para proporcionar una armonización mínima y para que los Estados miembros puedan ofrecer salvaguardias más elevadas para la protección de datos. Los diferentes niveles de normas de protección en la Unión dificultarán el intercambio de información y obstaculizarán la cooperación entre las autoridades competentes. El SEPD hace referencia al artículo 16 del TFUE, que establece que la Unión debe cuidar los altos estándares de protección de datos y no puede dejarlos sólo a los Estados miembros. El SEPD considera que la nueva Directiva no armoniza el campo tanto como lo haría el RGPD si también incluyera el ámbito cubierto por la Directiva, y que la Directiva deja demasiado margen para la interpretación de sus normas por parte de los Estados miembros. EDPS (2015b), Opinion 6/2015 A further step towards comprehensive EU data protection, 28 October 2015, págs. 4-5.

151. En fin, con respecto a la Directiva (UE) 2016/680, debe observarse que es *lex specialis* ("*specific rules*")[1605] en relación con el RGPD, por lo que sus principios y obligaciones se modulan en relación con el contexto específico de las actividades y los poderes de las autoridades policiales y judicial. Dado que las necesidades y circunstancias del tratamiento de datos personales no pueden preverse en detalle, la relación entre la Directiva y el Reglamento es importante. En particular, puede haber casos en los que las autoridades relacionadas con la seguridad participen en el tratamiento de datos personales que no estén contemplados en la Directiva sino en virtud del RGPD. Lo contrario también puede ocurrir: las agencias que normalmente llevan a cabo el tratamiento de datos personales de propósito general pueden encontrarse involucradas en el procesamiento ejecutado por motivos de seguridad. Con este fin, la Directiva aclara que sus disposiciones se aplican estrictamente en relación con el tratamiento de los datos personales con los fines establecidos y también proporciona algunas orientaciones útiles, pero deja el asunto a los Estados miembros para definirse mejor en la legislación nacional. Esta característica no puede ser ignorada en el proceso de transposición nacional, garantizando las conexiones necesarias con el RGPD[1606] e interviniendo en las reglas ya en vigor con vistas a la simplificación y la armonización.

152. En el presente apartado se analizan los límites de la nueva Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo con respecto a la protección del derecho individual a la privacidad cuando las autoridades nacionales tratan datos personales; los principales cambios al tratamiento de datos personales que la Directiva traerá consigo; las limitaciones a los derechos y libertades de la persona; y las transferencias de datos personales a terceros países u organizaciones internacionales por las autoridades competentes. A partir del análisis

[1605] Paul DE HERT, Vagelis PAPAKONSTANTINOU (2014b), *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, pág. 7. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510001/IPOL_STU(2014)510001_EN.pdf [consulta: 28 de mayo de 2017].

[1606] La Comisión Europea ha publicado unas orientaciones para facilitar una aplicación directa y fluida de las nuevas normas de protección de datos en toda la UE a partir del 25 de mayo de 2018. Las orientaciones resumen es lo que le queda por hacer a la Comisión Europea, a las autoridades nacionales de protección de datos y a las administraciones nacionales para que la preparación concluya de manera satisfactoria. Aunque el nuevo Reglamento prevé un conjunto único de normas directamente aplicables en todos los Estados miembros, todavía requerirá ajustes importantes en determinados aspectos, tales como la modificación de las leyes vigentes por los Gobiernos de la UE. En este momento, sólo dos de ellos (Austria y Alemania) han adoptado ya la legislación nacional pertinente. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018, COM(2018) 43 final, Bruselas, 24.1.2018. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52018DC0043 [consulta: 18 de febrero de 2018].

de la Directiva desde estos ángulos se puede adelantar que, aunque es una mejora considerable y un gran paso adelante para la protección de datos personales en ese ámbito, es poco probable que pueda arreglar la fragmentación del marco legal y lograr el alto nivel deseado de estándares de protección de datos consistentes en todos los Estados miembros de la Unión Europea.

4.1. El ámbito de la Directiva: abordar las deficiencias del pasado dejando al margen a los servicios secretos y las agencias de la UE

153. Unos de los primeros aspectos que se destacan en la Directiva (UE) 2016/680 es la importancia que tiene la tecnología junto con las autoridades policiales y judiciales en la lucha contra el terrorismo nacional e internacional, y más en general en la delincuencia: «*La rápida evolución tecnológica y la globalización han planteado nuevos retos en el ámbito de la protección de los datos personales. Se ha incrementado de manera significativa la magnitud de la recogida y del intercambio de datos personales* (…) *en una escala sin precedentes para la realización de actividades como la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales*»[1607]. Y luego la plena conciencia que «*Debe ser facilitada la libre circulación de datos personales entre las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública en el seno de la Unión y la transferencia de estos datos personales a terceros países y organizaciones internacionales, al tiempo que se garantiza un alto nivel de protección de los datos personales. Estos avances exigen el establecimiento de un marco más sólido y coherente para la protección de datos personales en la Unión Europea, que cuente con el respaldo de una ejecución estricta*»[1608].

154. A partir de estas características debe recordarse, sin embargo, que el objetivo expresado por la Directiva es la "libre circulación de datos", tal y como figura también en su título, lo que no debe tenerse siempre presente. En efecto, la intención de la Directiva no es restringir el flujo de información entre las agencias involucradas en el procesamiento de datos personales relacionados con la aplicación de la ley dentro del mismo o incluso entre los diferentes Estados miembros. De hecho, ocurre todo lo contrario: al introducir un marco legal integral de protección de datos sobre cómo ejecutar dicho tratamiento e intercambiar

[1607] Considerando 3 de la DIRECTIVA (UE) 2016/680.
[1608] Considerando 4 de la DIRECTIVA (UE) 2016/680.

dichos datos personales, la Directiva tiene como objetivo institucionalizar y agilizar dichos flujos de datos. En otras palabras, el objetivo aquí es permitir, a través de la regulación, y no prohibir el tratamiento de datos personales en el contexto de la policía y la justicia penal en toda la UE.

155. Sin embargo, dado que los datos recogidos por razones de prevención y seguridad en un determinado país pueden ser transmitidos en el resto de Europa y en el extranjero, sin, al mismo tiempo, garantizar el derecho a la vida privada, se exige que los Estados miembros se comprometan a garantizar que sus autoridades policiales y judiciales cumplen, en el tratamiento de los datos personales de todos los individuos, los mismos niveles mínimos de protección. Y es precisamente el objetivo de la nueva Directiva europea que ya está en vigor y está a la espera de ser acogida en los distintos países de la UE el 6 de mayo de 2018[1609]: «*La presente Directiva establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública*»[1610]. Y a continuación están las obligaciones que, desde mayo de 2018, los Estados miembros deberán cumplir: «*a) proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y b) garantizar que el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión, en caso de que el Derecho de la Unión o del Estado miembro exijan dicho intercambio, no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*»[1611].

[1609] La Directiva ya está en vigor y en España se ha incluido en el Plan Anual Normativo 2018 del Gobierno. En el proyecto de ley de la LOPD se menciona una Ley Orgánica sobre el tratamiento de datos personales para fines policiales y judiciales penales. *Vid*. GOBIERNO DE ESPAÑA, *Plan Anual Normativo 2018*, pags. 14 y 25. Italia, ha adoptado, a partir del 08/06/2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. DECRETO LEGISLATIVO 18 maggio 2018, n. 51. Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (*GU Serie Generale* n. 119 del 24-05-2018).

[1610] Artículo 1 (Objeto y objetivos), apartado 1, de la DIRECTIVA (UE) 2016/680.

[1611] Artículo 1, apartado 2, de la DIRECTIVA (UE) 2016/680. Con el fin de facilitar el intercambio "eficaz" de datos personales, los Estados miembros forman parte de la Organización Internacional de Policía Criminal (Interpol), que «*recibe, almacena y distribuye datos personales para ayudar a las autoridades competentes a prevenir y combatir la delincuencia internacional*». Por ello, conviene reforzar la cooperación entre la Unión e Interpol y del mismo modo que se «*garantiza el respeto de los derechos y libertades fundamentales en relación con el tratamiento automatizado de los datos personales*». Cuando se transmitan datos desde la Unión

156. La normativa europea, "busca uniformizar el nivel de protección de los derechos de las personas físicas en los Estados miembros en relación con el tratamiento de sus datos personales y facilitar el intercambio de datos entre las autoridades competentes de los Estados miembros". El objetivo es permitir una cooperación judicial efectiva en materia penal, aunque esta materia entra en la soberanía de los Estados miembros[1612].

157. Por lo tanto, "la protección de los datos personales debe garantizarse igualmente en todas partes en la UE". Bajo este sentido, el intento de la nueva Directiva es facilitar la realización de un ELSJ[1613], armonizando las legislaciones de los Estados miembros en este área. La Directiva establece el nivel mínimo[1614] de regulación declarando en casi todos los artículos que los Estados miembros "deben proporcionar" ciertas disposiciones en su legislación nacional, garantizando que el nivel de protección de los derechos de las personas naturales sea igual en todos los Estados miembros en relación con el tratamiento de sus datos personales por parte de las autoridades públicas nacionales[1615].

158. Mediante la Directiva, las instituciones de la UE permiten que los datos personales fluyan libremente entre las autoridades nacionales, para prevenir, investigar y enjuiciar delitos o ejecutar sanciones penales. El objetivo es prevenir las amenazas a la seguridad pública y transferir los datos personales a terceros países y organizaciones internacionales. Debe mantenerse un alto nivel de protección de los datos personales, sin que este dependa de las técnicas usadas o de los instrumentos de las autoridades[1616].

159. A este respecto debe tenerse en cuenta que la Directiva se aplica al tratamiento por parte de las autoridades nacionales competentes de los datos personales automatizados, así «*como al tratamiento no automatizado de datos personales*», para los fines mencionados

a Interpol y a los países que hayan destinado miembros a dicha organización, resultará de aplicación la Directiva. Considerando 25 de la DIRECTIVA (UE) 2016/680.

[1612] El SEPD, apoyando el instrumento de la Directiva, declaró que las normas son coherentes con el RGPD y que el nivel de protección garantizado por la Directiva está al menos al mismo nivel que el actualmente garantizado por otras leyes e instrumentos de la UE. El SEPD quiere que las autoridades de investigación sean efectivas en el futuro y que el intercambio de información sin problemas entre las autoridades es ahora más importante que nunca. Una discusión multidisciplinaria es una prioridad debido a los conocimientos técnicos requeridos en este campo, se necesita una mejor cooperación para mantener un enfoque basado en los derechos humanos. Todos, políticos, autoridades públicas, empresas, académicos, técnicos y personas deben cooperar para que el tratamiento de dados sea confiable. Vídeo del SEPD Giovanni Buttarelli, «EU Data Protection Reform: The Directive on police, justice and criminal matters», en *Youtube*, video, 7.12.2015. Disponible en Internet: https://www.youtube.com/watch?v=_Q19JtF3ieI&feature=youtu.be [consulta: 01 de junio de 2017].

[1613] Considerando 2 de la DIRECTIVA (UE) 2016/680.

[1614] Los Estados miembros deben proporcionar al menos el mismo nivel de protección en sus legislaciones.

[1615] Considerando 7 de la DIRECTIVA (UE) 2016/680.

[1616] Considerando 4 de la DIRECTIVA (UE) 2016/680.

anteriormente y al tratamiento de dichos datos[1617]. Por consiguiente, sus normas se aplican a todo tipo de trato, ya sea automatizado o manual. La introducción de tratamientos manuales ya había sido reconocida en la Decisión Marco 2008/977/JAI[1618] y constituye un progreso con respecto a las disposiciones del Convenio n. 108 y de la Recomendación 87 (15) del Consejo de Europa, que se aplican únicamente al tratamiento automatizado de datos. El mismo criterio se encuentra en el RGPD, que también contempla ambos tipos de tratamiento[1619].

160. Con esta Directiva se supera uno de los principales límites señalados en la Decisión Marco. De hecho, ahora el espacio de aplicación ya no se limita al trato transfronterizo, sino a las diversas actividades como la «*recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*»[1620], de datos personales contenidos o destinados a ser incluidos en un fichero, también se aplican al trato puramente nacional[1621]. Por lo tanto, por primera vez, el tratamiento transfronterizo de datos y trato nacional se unen en una única reglamentación.

161. A pesar del amplio enfoque que tiene la Directiva de protección de datos en los sectores policial y judicial, en lo que se refiere al ámbito de aplicación de la Directiva, su alcance real es más limitado de lo que parece a primera vista.

162. En primer lugar, su ámbito de aplicación se encuentra limitado al «*tratamiento de datos personales por parte de las autoridades competentes*» para los «*fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales*» (artículo 1), que no implique el tratamiento de datos personales en el contexto de los procedimientos penales[1622]. La «*autoridad competente*» puede a su vez ser autoridad pública («*las autoridades judiciales, la policía u otras fuerzas y cuerpos de*

[1617] Artículo 2 (Ámbito de aplicación), apartados 1 y 2, de la DIRECTIVA (UE) 2016/680.
[1618] En este sentido, DECISIÓN MARCO 2008/977/JAI, artículo 1 (Objetivo y ámbito de aplicación), apartado 3: «*La presente Decisión Marco se aplicará tanto al tratamiento automatizado como no automatizado, total o parcial, de datos personales que formen parte o esté previsto que vayan a formar parte de un fichero*».
[1619] *Cfr*. artículo 2 (Ámbito de aplicación material) del REGLAMENTO (UE) 2016/679.
[1620] Artículo 3 (Definiciones) de la DIRECTIVA (UE) 2016/680.
[1621] Artículo 2 de la DIRECTIVA (UE) 2016/680.
[1622] La Directiva (UE) 2016/680 no se aplica, como especifica su considerando 20, a los tratamientos de datos personales en el contexto de un procedimiento judicial penal, dejando que «*los Estados miembros especifiquen operaciones y procedimientos de tratamiento relativos al tratamiento de datos personales por parte de tribunales y otras autoridades judiciales*».

seguridad»), y "cualquier otro organismo o entidad" encargada por la legislación nacional del Estado de ejercer "la autoridad y las competencias públicas" a los efectos de la Directiva[1623]. En otras palabras, cuando los datos personales se tratan en el curso de una investigación penal y en procedimientos de materia penal, los Estados miembros podrán prever «*el ejercicio de los derechos de información, acceso*» y «*rectificación o supresión*» de los datos personales que se lleve a cabo de acuerdo con su legislación nacional[1624]. El derecho del interesado a obtener la rectificación, supresión o limitación del tratamiento puede ser limitado por los Estados miembros, mediante medida legislativa «*necesaria y proporcional en una sociedad democrática*» y teniendo en cuenta «*los derechos fundamentales y los intereses legítimos de la persona física afectada*», en caso de que sea necesario proteger, entre otros, la seguridad pública y la seguridad nacional[1625].

163. Por otro lado, la Directiva no regula el tratamiento de datos en el ejercicio de actividades no comprendidas «*en el ámbito de aplicación del Derecho de la Unión, por parte de las instituciones, órganos u organismos*» de la Unión[1626]. Esta disposición ha sido interpretada en relación con «*las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional y las actividades de tratamiento de datos personales que lleven a cabo los Estados miembros en el ejercicio de las actividades incluidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea (TUE)*»[1627]. Así que, se excluyen de su ámbito de aplicación las actividades concernientes: la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional; y las actividades de tratamiento de datos personales realizadas por los Estados miembros en el ejercicio de las

[1623] Considerando 11 de la DIRECTIVA (UE) 2016/680. *Cfr*. artículo 3 (Definiciones), núm. 7: «*autoridad competente*»: «*a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública*».

[1624] Considerando 49 de la DIRECTIVA (UE) 2016/680. Se recogen los principios que han de cumplir los Estados miembros en el tratamiento de datos personales, debiendo fijar «*plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Las normas de procedimiento garantizarán el cumplimiento de dichos plazos*». Artículo 5 (Plazos de conservación y revisión) de la DIRECTIVA (UE) 2016/680. En la misma línea, también vid. artículo 14 (Derecho de acceso del interesado a los datos personales) *infra*, y artículo 16 (Derecho de rectificación o supresión de datos personales y limitación de su tratamiento) de la DIRECTIVA (UE) 2016/680.

[1625] *Vid*. artículo 16, apartado 4, letra c) y d), de la DIRECTIVA (UE) 2016/680.

[1626] Artículo 2, apartado 3, de la DIRECTIVA (UE) 2016/680.

[1627] Considerando 14 de la DIRECTIVA (UE) 2016/680.

actividades comprendidas en el ámbito de aplicación sobre la política exterior y de seguridad común.

164. Aunque el alcance de la Directiva tiene límites, con respecto a estos primeros aspectos más salientes, ante todo hay que reconocer que la norma europea es el primer instrumento que armoniza las normas para el tratamiento de datos realizado por los Estados miembros en ámbito "policía y justicia", mediante la creación de ciertas limitaciones para los legisladores nacionales, armonización que es verificable por la Comisión y por el TJUE. En este sentido, por lo tanto, el verdadero valor añadido de la Directiva de protección de datos en los sectores de policía y justicia depende de su puesta en práctica en la legislación nacional y de la actividad de los tribunales nacionales para garantizar que la norma europea sea aplicada de manera uniforme en toda la UE[1628]. También hay que señalar que la Directiva es innovadora ya que su alcance está destinado a cubrir todo el tratamiento de datos personales, realizados en el marco de la cooperación policial y judicial en materia penal, con independencia de si el tratamiento se lleva a cabo dentro o fuera de las fronteras nacionales. En consecuencia, las autoridades competentes, por lo tanto, ya no tendrán que aplicar diferentes normas de protección de datos en función del origen de los datos personales.

165. Desafortunadamente, las ambigüedades existentes con respecto al ámbito de aplicación de la Directiva no se acaban aquí, ya que no se expresa con claridad lo que se entiende «*en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión*»[1629]. El término puede interpretarse de manera diferente en cada Estado de la UE y no prever una clara delimitación de las tareas de la policía dentro del ámbito de la Directiva. Hasta que el TJUE no haga una interpretación sobre este concepto, el ámbito de aplicación de la Directiva de protección de datos en los sectores de la policía y la justicia dependerá, de nuevo, de la interpretación que los tribunales nacionales puedan dar a la expresión "actividad no comprendida en el ámbito de aplicación del Derecho de la Unión", y de la forma en que los Estados miembros decidan aplicar la Directiva. Por otra parte, como se ha señalado anteriormente, el hecho de que las agencias de la UE que operan dentro el ELSJ no estén sujetas a las normas establecidas en la Directiva de protección de datos en los sectores policial y judicial crea un problema de coordinación entre las reglas establecidas en la Directiva y los contenidos en cada texto constitutivo de las mismas agencias.

[1628] La Directiva (UE) 2016/680 es aplicable a las «*personas físicas, independientemente de su nacionalidad o lugar de residencia*», en lo que se refiere al tratamiento de sus datos personales. *Vid*. considerando 17.
[1629] Artículo 2, apartado 3, letra a) de la DIRECTIVA (UE) 2016/680.

166. Como se ha podido comprobar, en la Directiva existen limitaciones importantes. En primer lugar, no hace referencia a los regímenes jurídicos de los organismos europeos implicados en la justicia criminal y policial (como, por ejemplo, Europol y Eurojust, y tampoco al *SIS* que, a diferencia de la Decisión Marco sí hace referencia). Esto significa que, por ejemplo, los datos tratados por Europol o Eurojust no entran dentro del alcance de la nueva Directiva[1630]. Tampoco regula bien la información personal que habitualmente intercambian entre ellos y con terceros países u organizaciones internacionales. En este sentido, el nuevo Reglamento (UE) 2018/1725, que deroga el Reglamento (CE) n. 45/2001, se pone como objeto de someter a estas agencias a un sistema de supervisión estricta, combinaría la protección de datos interna, comisiones mixtas y la supervisión de SEPD[1631].

167. En segundo lugar, es parcialmente contradictoria y poco clarificadora la formulación de las disposiciones contenida en "objeto y objetivos" por el artículo 1, apartado 1, de «*la protección y la prevención frente a las amenazas contra la seguridad pública*»[1632]. Esto causa problemas interpretativos, ya que el concepto a examen se presta a diversas actividades y diferentes interpretaciones. Incluso, no se define en el texto de manera clara y precisa qué se entiende por actividades relacionadas con la seguridad pública, así que parece que no se incluye la totalidad de las actividades de protección y de prevención de amenazas a la

[1630] La Directiva, aunque excluye las transferencias de datos de Europol de su alcance jurídico, tiene un claro impacto directo sobre el Reglamento de Europol. En este sentido, el considerando 40 del Reglamento Europol resalta la importancia de alinear ambos textos jurídicos: «(…) *las normas de protección de datos de Europol deben ser autónomas y al mismo tiempo coherentes con otros instrumentos pertinentes en materia de protección de datos aplicables en el ámbito de la cooperación policial en la Unión. Dichos instrumentos incluyen, en particular, la Directiva (UE) 2016/680 del Parlamento Europeo y de del Consejo, así como el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Recomendación n.º R(87) 15*». Se debe tener en cuenta que la principal fuente de obtención de información de Europol es a través de los Estados miembros, que deben seguir las normas de protección de datos de la nueva Directiva, Así pues, tiene sentido que el hecho de que la Directiva se demorara tanto en aprobarse retrasó también la votación en el Consejo y en el Parlamento para la adopción del Reglamento de Europol. Cristina BLASI CASAGRAN (2016b: 215).

[1631] Paul DE HERT, Vagelis PAPAKONSTANTINOU (2014b: 37). El procesamiento de datos por las instituciones y organismos europeos continuará rigiéndose por el nuevo REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. 45/2001 y la Decisión n. 1247/2002/CE.

[1632] En el proceso de redacción del proyecto de la Directiva de protección de datos en materia policial, el Consejo de la UE incluyó la frase «*o de protección y prevención frente a las amenazas contra la seguridad pública*», como motivo para interferir con los derechos de las personas. Esta «*prevención frente a las amenazas contra la seguridad pública*» puede interpretarse como básicamente cualquier cosa que la actual autoridad pública nacional considere amenazante, ya sea una amenaza o no. Sin embargo, esta frase fue incluida en el texto final. *Vid*. PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a los datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de protección de las personas físicas en lo que respecta al tratamiento de dichos datos − Orientación general, 12555/15, Bruselas, 2 de octubre de 2015, pág. 5. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/es/pdf [consulta: 06 de junio de 2017].

seguridad pública: «*Las actividades realizadas por la policía u otras fuerzas y cuerpos de seguridad se centran principalmente en la prevención, investigación, detección o enjuiciamiento de infracciones penales, incluidas las actuaciones policiales en las que no hay constancia de si un incidente es o no constitutivo de infracción penal. También pueden incluir el ejercicio de la autoridad mediante medidas coercitivas, como es el caso de las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios. Entre dichas actividades también figura el mantenimiento del orden público, como labor encomendada a la policía o, en su caso, a otras fuerzas y cuerpos de seguridad con fines de protección y prevención frente a las amenazas para la seguridad pública y para los intereses públicos fundamentales jurídicamente protegidos que puedan ser constitutivas de infracciones penales*»[1633]. También, los Estados miembros pueden conferir a las autoridades competentes otras funciones que no se realicen necesariamente para prevenir, investigar, detectar o enjuiciar infracciones, incluida la protección contra las amenazas a la seguridad pública y su prevención, de modo que el trato de datos personales con estos otros fines, en la medida en que recaen en el ámbito de aplicación del Derecho de la Unión, está sujeto a las normas más estrictas del RGPD[1634]. Además, tenemos que añadir que la "seguridad pública" y la "seguridad nacional" son conceptos en evolución, elásticos y mutantes cuyo alcance depende del momento histórico de referencia, por lo que sus significados no deberían estar escritos de manera demasiado estricta en la ley o podrían limitar la capacidad de adaptación a través de la interpretación de las autoridades.

168. Por último, el fin que pretende la Directiva de garantizar la máxima armonización europea de tratamiento de datos en el ámbito penal, todavía está lejos de conseguirse. Así se confirma en el artículo 1, apartado 3, que establece que la norma «*no impedirá a los Estados miembros ofrecer mayores garantías que las que en ella se establecen para la protección de*

[1633] Considerando 12 de la DIRECTIVA (UE) 2016/680.

[1634] El RGPD establece reglas generales «*para garantizar la libre circulación de datos personales*» y «*para proteger a las personas físicas en relación con el tratamiento de datos personales*» dentro de la UE. La nueva Directiva y el RGPD se complementan entre sí, ya que operan en diferentes sectores, pero cooperan en las áreas donde se superponen. Por ejemplo, si los datos personales fueron coleccionados por una autoridad competente para uno de los fines de la Directiva, el RGPD debería aplicarse al tratamiento de tales datos para finalidades diferentes de los de la Directiva, si dicho procesamiento está autorizado por el Derecho de la Unión o del Estado miembro. En particular, las normas del RGPD deberían «*aplicarse a la transmisión de datos personales para fines que no entran en el ámbito de aplicación de la Directiva*». En el tratamiento de los «*datos personales por parte de un destinatario que no sea una autoridad competente*» o que no ejerza esta función con arreglo a la Directiva y a «*quien una autoridad competente*» divulgue lícitamente datos personales, se debería aplicar el RGPD. Al aplicar la Directiva, los Estados miembros deberían poder especificar mejor la aplicación de las normas del RGPD, «*con sujeción a las condiciones establecidas en el mismo*». Considerando 34 de la DIRECTIVA (UE) 2016/680. El SEPD afirmó que la protección de datos en los sectores policiales debería ser coherente con las reglas generales escritas en la propuesta de RGPD y especificarse sólo si es necesario. EDPS (2015b: 4-5).

los derechos y libertades del interesado con respecto al tratamiento de datos personales por parte de las autoridades competentes». La propuesta de Directiva no contemplaba dicho apartado, a pesar de que algunos Estados miembros ya habían expresado públicamente su voluntad de ofrecer garantías de protección de datos más altas a nivel nacional que las que incluye la propuesta. Este apartado es un trasunto del artículo 1, apartado 5, de la Decisión Marco 977/2008/JAI[1635]. La Directiva permite a los Estados miembros la posibilidad de proporcionar garantías mayores, lo que constituye un aspecto importante para la protección de los derechos fundamentales, considerando que la discusión de los avances realizados en el Consejo[1636] llevó a una nueva redacción de los artículos, en particular, relativos a los derechos de los interesados que, proporcionando un mayor número de excepciones, amenaza de comprimir el ejercicio efectivo de los derechos de información, acceso, rectificación y cancelación de datos (*infra*). Por consiguiente, esto deja un amplio margen de maniobra a los Estados en la definición de las categorías de tratamiento, el riesgo relativo y las normas resultantes. La Directiva prevé, en efecto, que sea dada una información muy general sobre el tratamiento, y deja al legislador nacional especificar los casos en que tenga que ser información más detallada, con el fin de salvaguardar las investigaciones y otros aspectos de interés público.

4.2. Principios y legalidad del tratamiento de datos personales

169. La Directiva de protección de datos en materia policial repite los principios de la normativa de protección de datos ya establecida en la Directiva de 1995[1637]. La diferencia es, como ya se ha indicado, que, por primera vez, la Unión ordena que estos principios se apliquen también en el ámbito policial. Por ello, el tratamiento de los datos personales debe ser: "lícito y leal"; "recopilados para fines determinados, explícitos y legítimos y no procesados de manera incompatible con esos fines"; "adecuado", "pertinentes y no excesivos en relación con los fines para los que se procesan"; "exactos" y, cuando sea necesario, "actualizados"; "deben tomarse todas las medidas razonables para garantizar que los datos personales que sean inexactos", teniendo en cuenta los fines para los que se tratan, se borren o rectifiquen sin demora; "conservados en una forma que permita la identificación de los interesados por un período no superior al necesario para los fines para los que se

[1635] Esta cláusula prevé que la Decisión Marco no impida que los Estados miembros puedan adoptar estándares más altos de protección de datos que los establecidos a nivel europeo: «*La presente Decisión Marco no impedirá a los Estados miembros establecer, para la protección de los datos personales recopilados o tratados a nivel nacional, garantía mayores a las establecidas en la presente Decisión Marco*».
[1636] PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 14901/2/13, REV 2.
[1637] DIRECTIVA 95/46/CE, artículo 6.

tratan"; "procesados de manera que garantice la seguridad adecuada de los datos personales, incluida la protección contra el procesamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental, utilizando medidas técnicas u organizativas apropiadas"[1638]. Con el objetivo de garantizar que los datos no se almacenen más de lo necesario, el responsable de los datos debe establecer un plazo para la supresión o la revisión periódica. Las personas deben ser informadas de los posibles riesgos, reglas, salvaguardas y «*derechos aplicables en relación con el tratamiento de sus datos personales y del modo de hacer valer sus derechos*»[1639]. El responsable del tratamiento de datos debe demostrar que cumple con las reglas establecidas anteriormente[1640].

170. El principio de finalidad es un aspecto fundamental de todos los instrumentos que regulan el intercambio de información. La limitación de los fines se refleja, más allá de los límites de la utilidad de la información, también sobre el tipo de datos personales que pueden ser recopilados e intercambiados y sobre la identificación de las autoridades autorizadas para acceder. Podemos derivar de ello dos aspectos principales: los datos sólo deben usarse para fines limitados y sólo deben conservarse durante un tiempo limitado. Los datos personales almacenados deben revisarse y borrarse periódicamente después de los límites de tiempo apropiados[1641].

171. Estos aspectos, sin embargo, plantean equívocos por lo que respecta el artículo 4, apartado 1. La forma correcta de interpretar el artículo no es clara y no debería trasladarse directamente en la ley nacional antes de que se hayan delimtiado su contenido a través de la interpretación del TJUE. La nueva Directiva permite, también a este respecto, amplias posibilidades a los Estados miembros para interpretar las disposiciones. También se reconoce que «*Los Estados miembros dispondrán que los datos personales sean:* (…) *e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados* (…)»[1642]. El riesgo que puede derivarse de este redactado es que la información termine usándose para múltiples procedimientos de

[1638] Artículo 4 (Principios relativos al tratamiento de datos personales), apartado 1, de la DIRECTIVA (UE) 2016/680.
[1639] Considerando 26 de la DIRECTIVA (UE) 2016/680. Los Estados miembros deberían «*establecer salvaguardias adecuadas para los datos personales*» mantenidos «*durante períodos más largos*» a fin de archivarlos por cuestiones de interés público o con fines científicos, históricos o estadísticos.
[1640] Artículo 4, apartado 4, de la DIRECTIVA (UE) 2016/680.
[1641] Artículo 5 (Plazos de conservación y revisión) de la DIRECTIVA (UE) 2016/680.
[1642] Artículo 4, apartado 1, de la DIRECTIVA (UE) 2016/680.

investigación sin ningún tipo de limitación temporal[1643]. Además, el Grupo de Trabajo, ya en su opinión sobre el proyecto de reforma de 2012, denunciaba la falta de cualquier indicación de limitaciones temporales de almacenamiento de datos o incluso en relación con revisiones regulares de la necesidad de seguir la conservación de la información previamente adquirida[1644]. En este contexto, la sentencia de anulación de la Directiva de conservación de datos de 2006 por el TJUE en el 2014 ha despertado mucho debate[1645] en relación con la falta de normas precisas sobre la cooperación entre entes públicos y privados en las medidas de "elaboración de perfiles"[1646].

172. La tendencia actual en Europa es que las autoridades traten de recopilar una mayor cantidad de datos[1647]. Las autoridades ya tienen acceso a una gran cantidad de datos, pero el problema es que aún no hay suficientes recursos para analizar todos esos datos por lo que siempre es necesario contar con más tiempo[1648]. Se trata de la necesidad de encontrar un equilibrio adecuado entre la seguridad y la privacidad que se deriva de la previsión del tiempo y modalidad de conservación de los datos razonables y proporcionadas a las necesidades de la investigación de los delitos más graves. Al mismo tiempo, hay que respetar el principio de proporcionalidad respecto al que el TJUE ha modulado el equilibrio entre la libertad y la seguridad, subrayando la necesidad de una adecuada selección de material de investigación, lo que ciertamente no puede ser *sui géneris*. Cuando las autoridades piden más herramientas para recopilar datos personales, primero deben evaluarse las herramientas ya existentes para determinar si son o no efectivas.

173. En el ELSJ, donde hay un aumento continuo de flujos común de datos, la cooperación e intercambio de información es una exigencia fundamental[1649]. La Directiva

[1643] PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 14901/2/13, REV 2, pág. 6.
[1644] ARTICLE 29 DATA PROTECTION WORKING PARTY (2012b).
[1645] Franziska BOEHM, Mark D. COLE (2014: 85-87).
[1646] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 27: «*Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan*».
[1647] El tema está de actualidad también debido a la reciente adopción en Francia de una nueva ley sobre el control de las comunicaciones electrónicas internacionales, después de los acontecimientos de París del 13 de noviembre de 2015 (teatro Bataclan), que amplía los poderes del ejecutivo en materia de adquisición de datos, sin previa autorización ni control judicial.
[1648] La respuesta correcta sería no recopilar, por ejemplo, el ADN de todos en archivos policiales, sino que la medida debe ser proporcional ya que el ADN de personas inocentes no debe figurar en los archivos policiales.
[1649] Desafortunadamente, no es así como, en realidad, las cosas funcionan. Un ejemplo es la escasa y tardía colaboración entre las autoridades de seguridad de Bélgica y Francia después de la matanza en París del 7 de enero de 2015 en la sede del diario *Charlie Hebdo*.

de 2016 proporciona reglas significativas para la aplicación del "principio de limitación de la finalidad", puesto que la Directiva parece que tiene capacidad para el uso de grandes volúmenes de datos por aplicación de la ley y la actuación de métodos de control de datos por parte de la inteligencia a través de amplias excepciones al principio de finalidad, reconocidos en el artículo 4, apartado 2. De hecho, se permite el tratamiento de los datos personales, por el mismo responsable o por otro, para cualquiera de los fines mencionados en el artículo 1, apartado 1 (es decir: prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública), diferentes de aquel para el que se recopilan los datos personales, «*en la medida en que el responsable del tratamiento de datos esté autorizado a procesar dichos datos personales*» a tal efecto de conformidad con el Derecho de la Unión o del Estado miembro, y «*el tratamiento es necesario y proporcionado a ese otro fin*» de conformidad con la legislación de la Unión o del Estado miembro[1650]. Para otros fines, se aplican las reglas del RGPD.

174. Sin embargo, la Directiva incluye unas exigentes obligaciones de transparencia por lo que respecta a la utilización de "registro de operaciones"[1651] y requiere que el intercambio de datos sea proporcional[1652]. Las autoridades de control, fomentando una «*cooperación más estrecha entre las autoridades de control de la protección de datos a fin de contribuir al intercambio de información*»[1653], deberían aprovechar para instalar un "control estrecho"

[1650] *Cfr*. artículo 4, apartado 2, de la DIRECTIVA (UE) 2016/680.

[1651] Artículo 25 (Registro de operaciones) de la DIRECTIVA (UE) 2016/680. Las autoridades competentes deben mantener los registros de «*las operaciones de tratamiento*» que se llevan a cabo en los sistemas de procesamiento automatizado. Los registros deben mantenerse al menos para la «*recogida, alteración, consulta y comunicación, incluidas las transferencias, combinación o supresión*». La Directiva establece que los registros de consulta y comunicación deben permitir determinar la «*fecha y hora*» de las operaciones, su justificación y, «*en la medida de lo posible*», la identificación de la persona que consultó el sistema o divulgó los datos personales, y destinatarios de los datos personales afectados. Los registros se deben utilizar sólo con el objetivo «*de verificar la legalidad del tratamiento*», para «*el autocontrol*», para «*garantizar la integridad*» y seguridad de los datos personales y para los procesos penales. A solicitud de la autoridad supervisora, el responsable y el encargado deben poner a su disposición los registros. Considerandos 56 y 57 de la DIRECTIVA (UE) 2016/680.

[1652] Los objetivos de la Directiva (artículo 1), no pueden lograrse de manera suficiente por los Estados miembros, sino que, debido al alcance y los efectos de la acción en cuestión, pueden lograrse mejor a nivel de la Unión, ésta puede intervenir sobre la base del principio de subsidiariedad consagrado en el artículo 5 del TUE. La Directiva «*no excede de lo necesario para alcanzar*» estos objetivos de conformidad con el principio de proporcionalidad enunciado en el mismo artículo. *Vid*. considerando 93 de la DIRECTIVA (UE) 2016/680.

[1653] Considerando 74 de la DIRECTIVA (UE) 2016/680. El intercambio de datos e información entre las autoridades policiales y judiciales de los distintos Estados miembros representa –y el tema es muy relevante hoy en día, especialmente después de los dramáticos acontecimientos terroristas– una herramienta indispensable para garantizar la seguridad en Europa. Un ejemplo concreto de este tipo de sinergia, con el fin de mejorar la seguridad de los ciudadanos en el ELSJ, como ya hemos tenido ocasión de analizar, es la extensión de la eficacia del Sistema Europeo de Información de Antecedentes Penales conocido como *ECRIS* (*European Criminal Records Information System*), que permite el intercambio de información de los registros de antecedentes penales, de una manera rápida, uniforme y fácilmente transferible por ordenador, entre los

sobre el intercambio de información entre las autoridades policiales, con el fin de «*supervisar la aplicación de las disposiciones adoptadas en aplicación de la presente Directiva y deben contribuir a su aplicación coherente en toda la Unión, con el fin de proteger a las personas físicas en relación con el tratamiento de sus datos personales. Para ello, las autoridades de control deben cooperar entre sí y con la Comisión*», como expresado por el considerando 75.

175. Los datos personales basados en hechos deben separarse de los datos que se basan en apreciaciones personales. Las autoridades competentes no deberían poner a disposición ni transmitir datos personales inexactos e incompletos y deberían verificar la calidad de los datos antes de su trato[1654]. Cuando los datos personales se envían a otras autoridades, «*la autoridad competente receptora*» debe «*valorar en qué medida los datos personales son exactos, completos y fiables y si están actualizados*»[1655]. Si se transmiten datos personales incorrectos o de forma ilegal, el destinatario debe ser puesto en conocimiento y los datos deben rectificarse o suprimirse o restringirse el tratamiento. También se establece en el artículo 6 la obligación del responsable de datos de establecer, «*en la medida de lo posible, una distinción clara entre datos personales*»: de personas para las cuales existen motivos fundados para presumir que han cometido o están a punto de cometer delitos; personas condenadas por un crimen; víctimas del crimen o personas a las que algunos hechos autorizan a considerar víctimas potenciales del crimen y los terceros involucrados. Aunque aún es pronto para determinar cómo esta separación se llevará a cabo en la práctica, las

países de la Unión Europea, en un formato europeo normalizado a través de una única consulta. El sistema permite acceder fácilmente a una información completa sobre el historial delictivo de cualquier ciudadano de la UE, con independencia de en qué países de la UE haya sido condenada dicha persona en el pasado. *Vid*. «Sistema Europeo de Información de Antecedentes Penales (ECRIS)», en *Portal Europeo de e-Justicia*. Disponible en Internet: https://e-justice.europa.eu/content_criminal_records-95-es.do [consulta: 11 de junio de 2017].

[1654] Con respecto a la calidad de los datos, ya la Decisión Marco 2008/977/JAI incluía la obligación de las autoridades de llevar a cabo un control de los datos como condición previa para la transmisión, asegurándose de que estos fueran precisos, completos y actualizados. Sin embargo, la Decisión Marco no preveía la diferenciación de los datos por categorías de datos, exactitud y la fiabilidad de la información, contrariamente a lo dispuesto en otros instrumentos normativos, como la Recomendación R (87) 15 o las Decisiones Europol y Eurojust. De hecho, la necesidad de establecer diferentes reglas de tratamiento para la información relativa a personas no implicadas en un proceso penal o absueltas, es una expresión de garantía fundamental, ya que una recopilación indiferenciada y un tratamiento generalizado en materia penal es muy perjudicial para la presunción de inocencia.

[1655] Artículo 7 (Distinción entre datos personales y verificación de la calidad de los datos personales) de la DIRECTIVA (UE) 2016/680. El apartado 2 del artículo, establece que la autoridad competente debe adoptar «*todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros*». El hecho de que esta cláusula sea tan general e incluso un tanto ambigua no es casualidad. Aunque en un primer borrador de la Directiva se incluían distintos niveles de veracidad y fiabilidad, éstos se eliminaron de la versión final precisamente porque entraban en conflicto con el artículo 29 del Reglamento de Europol, que establecía unos niveles de fiabilidad y exactitud diferentes. Cristina BLASI CASAGRAN (2016b: 215).

autoridades policiales nacionales tratarán los datos de manera diferente según la categoría de datos de que se trate.

176. El tratamiento de datos personales, para que sea lícito, en virtud de la Directiva "debe ser necesario" para la realización de «*una función de interés público llevada a cabo por una autoridad competente*» en virtud de la legislación de la UE o del Estado miembro «*con fines de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluida la protección y prevención de amenazas a la seguridad pública*»[1656]. Estas actividades deberían incluir salvaguardar los intereses vitales del interesado. El cumplimiento de estas funciones permite a las autoridades competentes «*exigir u ordenar a las personas que atiendan a las solicitudes que se les dirijan*». En esta situación, «*el consentimiento del interesado*», tal como se define en el RGPD, no debe constituir la base legal «*para el tratamiento de datos personales por parte de las autoridades competentes*» (considerando 35). Si se le exige cumplir con una obligación legal, la persona en cuestión no puede realizar una elección auténticamente libre, por lo tanto, su reacción no puede considerarse una manifestación libre de su voluntad.

177. Las autoridades competentes podrán tratar datos personales para fines distintos a los establecidos en el artículo 1, apartado 1, si cumplen las condiciones del artículo 9[1657]. En relación con el tratamiento de datos sensibles[1658], en línea con la Decisión Marco

[1656] Considerando 35 de la DIRECTIVA (UE) 2016/680.

[1657] Artículo 9 (Condiciones de tratamiento específicas) de la DIRECTIVA (UE) 2016/680: «*1. Los datos personales recogidos por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, no serán tratados para otros fines distintos de los establecidos en el artículo 1, apartado 1 salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento (UE) 2016/679 a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión. 2. Cuando el Derecho del Estado miembro encomiende a las autoridades competentes el desempeño de funciones que no coincidan con los fines establecidos en el artículo 1, apartado 1, se aplicará el Reglamento (UE) 2016/679 al tratamiento con dichos fines, incluidos fines de archivo en interés público, de investigación científica e histórica o estadísticos, salvo que el tratamiento se lleve a cabo en una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión. 3. Los Estados miembros dispondrán que, cuando el Derecho de la Unión o del Estado miembro aplicable a la autoridad competente transmisora prevea condiciones específicas aplicables al tratamiento, la autoridad competente transmisora deberá informar al destinatario al que se transmitan los datos de las condiciones y la obligación de respetarlos. 4. Los Estados miembros dispondrán que la autoridad competente transmisora no aplique las condiciones del apartado 3 a los destinatarios de otros Estados miembros o a los organismos, agencias y órganos establecidos en virtud de los capítulos 4 y 5 del título V de la tercera parte del TFUE distintas de las aplicables a las transmisiones de datos similares en el Estado miembro de la autoridad competente transmisora*».

[1658] Una explicación sobre una especial protección de los "datos sensibles", es proporcionada por la DIRECTIVA (UE) 2016/680 en el considerando 37: «*Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento puede generar riesgos importantes para los derechos y las libertades fundamentales. Dichos datos personales deben incluir aquellos que pongan de manifiesto el origen racial o étnico, entendiéndose que el término «origen racial» empleado en la presente Directiva no implica la*

2008/977/JAI, pueden procesarse «*cuando sea estrictamente necesario*», «*con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado*» y exclusivamente cuando sea autorizado por el Derecho de la UE o del Estado miembro, «*para proteger los intereses vitales del interesado o de otra persona física*», o si el interesado de los datos ha hecho manifiestamente públicos los mismos[1659]. Con respecto a los datos sensibles, la regla general es "prohibir el tratamiento de todos los datos que revelen origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, condiciones de salud y vida sexual, excepto en el caso cuando sea estrictamente necesario y la legislación nacional brinde salvaguardias adecuadas". Aunque en el ámbito de la cooperación judicial y policial, a diferencia de las disposiciones de la Directiva 95/46/CE, no se requiere el consentimiento del interesado para permitir el procesamiento de datos. En términos de datos sensibles, la Directiva introduce dos innovaciones: una de forma, la otra de contenido. La formulación del artículo 10 resulta novedosa ya que no establece una prohibición, sino que establece "en general" la posibilidad de tratar datos sensibles cuando, como se mencionó anteriormente, sea estrictamente necesario, con sujeción a las garantías adecuadas de los derechos y libertades del interesado o si se autoriza por la legislación de la UE o del Estado miembro, o de otro modo, si es necesario para salvaguardar un interés vital del interesado u otra persona física. La segunda novedad consiste, en cambio, en haber incluido dentro del rango de datos sensibles también los genéticos y biométricos, destinados a identificar inequívocamente a una persona natural. A diferencia del RGPD, con respecto a los datos sensibles, incluido los datos biométricos, la Directiva establece que sólo es posible si es estrictamente necesario y con las garantías adecuadas de los derechos y libertades del individuo, pero no por razones relacionadas con la protección del interés público o la seguridad pública[1660].

178. El interesado de los datos «*debe tener derecho*» a no estar sujeto a «*una decisión que evalúe*» los «*aspectos personales que le conciernen*» exclusivamente basada al «*tratamiento automatizado*» y que produzca efectos jurídicos negativos en su contra o que

aceptación por parte de la Unión Europea de teorías que traten de determinar la existencia de razas humanas diferentes (…)».

[1659] Artículo 10 (Tratamiento de categorías especiales de datos personales) de la DIRECTIVA (UE) 2016/680.

[1660] Según el artículo 10, el tratamiento de datos personales «*que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente cuando: a) lo autorice el Derecho de la Unión o del Estado miembro; b) sea necesario para proteger los intereses vitales del interesado o de otra persona física, o c) dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos*». *Cfr*. artículo 9 del RGPD.

afectan significativamente a su persona[1661]. En cualquier caso, dicho tratamiento debe estar sujeto a «*medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento*»[1662]. Según los artículos 21 y 52 de la Carta queda "prohibida" la «*elaboración de perfiles*»[1663] que conduzca a la «*discriminación de las personas físicas*» basada en datos personales que, por su naturaleza, son particularmente sensibles en términos de derechos y libertades fundamentales[1664]. En consecuencia, se permite el uso de la información en el contexto de la policía y la justicia penal, incluso sobre la base de datos sensibles, sin perjuicio de las salvaguardias adecuadas para los derechos y las libertades de las personas.

179. Las elaboraciones de perfiles son especialmente problemáticas en el contexto de policía y justicia penal, ya que, "el abuso de perfiles produce efectos jurídicos negativos para el interesado o le afectan considerablemente", como ser puestos bajo vigilancia o detenidos por motivos de tratamiento automatizado de datos de carácter personal. Una cosa es crear perfiles para el procesamiento de datos personales con fines generales (que se utilizarán, por ejemplo, con fines de *marketing* o de gestión de clientes) y otra completamente distinta es crear perfiles que posteriormente se utilicen para la prevención y la investigación del delito. Si bien el ideal sería obviamente abolir ese procesamiento y juzgar a cada individuo por sus propios méritos y peculiaridades[1665], los organismos encargados de hacer cumplir la ley han sostenido durante mucho tiempo que el aprovechamiento, si se usa correctamente, es particularmente útil en el desempeño de sus funciones. Es necesario subrayar aquí que, a este respecto, la Directiva de protección de datos con fines de cooperación policial y judicial en materia penal ofrece garantías sustanciales y procesales[1666].

[1661] Considerando 38 de la DIRECTIVA (UE) 2016/680.
[1662] Artículo 11 (Mecanismo de decisión individual automatizado), apartado 1, de la DIRECTIVA (UE) 2016/680.
[1663] Sobre la "elaboración de perfiles", *vid*. artículo 3 (Definiciones) de la DIRECTIVA (UE) 2016/680: «*4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*».
[1664] Artículo 11, apartado 3, de la DIRECTIVA (UE) 2016/680: «*La elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales establecidas en el artículo 10 quedará prohibida, de conformidad con el Derecho de la Unión*».
[1665] Paul DE HERT and Vagelis PAPAKONSTANTINOU (2016: 16).
[1666] De hecho, «*los Estados miembros dispondrán la prohibición de las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o le afecten significativamente, salvo que estén autorizadas por el Derecho de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento y que establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento*». Artículo 11, apartado 1, de la DIRECTIVA (UE) 2016/680.

4.3. Restricciones a los derechos y libertades de la persona para proteger la seguridad pública

180. Una vez determinados el alcance y los límites de la Directiva de protección de datos en los sectores de policía y justicia, nos centraremos ahora en el análisis de los diferentes aspectos sobre la protección de datos y derechos de los interesados relacionados con la misma que resultan más relevantes al objeto de la presente investigación.

181. Con respecto a los principios relativos al tratamiento de los datos personales, varios de los que se contienen en la Directiva son los mismos que los consagrados en el RGPD. Sin embargo, debido a la peculiaridad de la materia, mientras que los principios básicos de protección de datos se incluyen en su texto, se incluyen otros principios que no figuran en el RGPD. En todo caso, los principios básicos del tratamiento (licitud, lealtad, transparencia y calidad de datos), el ejercer los derechos de los interesados «*en materia de información, acceso a los datos personales, rectificación o supresión de estos y limitación de su tratamiento* (…)»[1667] y la existencia de una autoridad específicamente responsable de asegurar el cumplimiento de la legislación, son pilares esenciales de la nueva Directiva, aunque con diferencias con respecto a las disposiciones del RGPD debido, como dicho, al particular ámbito disciplinado.

182. En concreto, la nueva Directiva tiene un Capítulo para los derechos de los interesados[1668]. Estos derechos contienen normas de información que deben estar disponibles para el interesado, su derecho de acceso a sus datos personales y las disposiciones sobre la limitación del derecho de acceso, el derecho a rectificar o suprimir sus datos o limitar el tratamiento, y sus derechos en los procesos penales. Además, la autoridad supervisora competente puede ejercer y verificar los derechos del interesado.

183. La Directiva incluye algunas mejoras con respecto a los derechos de los individuos, como la obligación de notificarles que sus datos personales son tratados[1669]. Se contemplan los derechos del interesado y su forma de ejercicio: información que se debe poner a su

[1667] Considerando 107 de la DIRECTIVA (UE) 2016/680.
[1668] Capítulo III (Derechos del interesado), artículos 12-18 de la DIRECTIVA (UE) 2016/680.
[1669] El artículo 14 de la Directiva, establece la obligación de los Estados miembros de garantizar el derecho del interesado a acceder a sus datos personales.

disposición[1670] y derecho de acceso, rectificación o supresión de sus datos personales, incluyendo sus limitaciones[1671].

184. Sin embargo, existen aún muchas excepciones con respecto al derecho a ser informado y al derecho de acceso a sus datos personales. En lo que respecta al derecho a la información[1672], cabe señalar que "la Directiva regula la posibilidad de adoptar excepciones a la obligación de información", dejando a la determinación de los Estados miembros de determinar «*medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información* (…) *siempre y cuando dicha medida constituya una medida necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para: a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas*»[1673].

185. En relación a las limitaciones al derecho de acceso a sus datos personales, a los Estados miembros se les reconoce la posibilidad de adoptar «*medidas legislativas por las que se restrinja, total o parcialmente, el derecho de acceso del interesado siempre y cuando dicha restricción parcial o completa constituya una medida necesaria y proporcional en una*

[1670] El artículo 12 de la DIRECTIVA (UE) 2016/680 introduce la obligación de los Estados miembros de facilitar al interesado toda información, así como cualquier comunicación «*relativa al tratamiento, en forma concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo*. *La información será facilitada por cualquier medio adecuado, inclusive por medios electrónicos*».

[1671] Artículo 14, letra e), de la DIRECTIVA (UE) 2016/680.

[1672] Artículo 13 (Información que debe ponerse a disposición del interesado o que se le debe proporcionar), apartado 1, de la DIRECTIVA (UE) 2016/680: «*Los Estados miembros dispondrán que el responsable del tratamiento de los datos ponga a disposición del interesado al menos la siguiente información: a) la identidad y los datos de contacto del responsable del tratamiento; b) en su caso, los datos de contacto del delegado de protección de datos; c) los fines del tratamiento a que se destinen los datos personales; d) el derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma; e) la existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o su supresión, o la limitación de su tratamiento*». Además de estos requisitos de información general, la Directiva establece que, en casos específicos, y para permitir el ejercicio de sus derechos, los responsables deben proporcionar a los interesados información sobre la base legal para el tratamiento y sobre cuánto tiempo se conservarán los datos. Si los datos personales se transmiten a otros destinatarios, incluso en terceros países u organizaciones internacionales, los interesados deben ser informados de las categorías de dichos destinatarios. Finalmente, los controladores deben proporcionar cualquier información adicional, tomando en cuenta las circunstancias específicas en las que se procesan los datos, por ejemplo, cuando se recopilaron datos personales durante la vigilancia encubierta, es decir, sin el conocimiento del sujeto de los datos. Esto garantiza un tratamiento justo con respecto al sujeto de datos. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).

[1673] Artículo 13, apartado 3, de la DIRECTIVA (UE) 2016/680. *Cfr*. considerando 44.

sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para: a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales; b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales; c) proteger la seguridad pública; d) proteger la seguridad nacional; e) proteger los derechos y libertades de otras personas»[1674].

186. Esto se debe a que el artículo 15 permite a "los Estados miembros pever medidas que restrinjann el derecho de acceso" de los interesados a sus datos, con una base para proteger la seguridad nacional. En estos casos, "es esencial aproximar la defensa de la seguridad en una sociedad democrática con la salvaguarda de los derechos individuales, tratando de encontrar un equilibrio entre las dos necesidades". En este sentido es muy importante cómo los Estados miembros aplicarán las excepciones contenidas en la Directiva en las leyes nacionales, es decir, si se respetará el justo equilibrio entre la protección de datos personales y los intereses de la policía y de proceso penal. Se puede decir que dichas limitaciones (de los derechos de información, acceso, rectificación y supresión)[1675] intentan así lograr un equilibrio entre el derecho individual a la protección de datos y los intereses de la policía y de otros organismos relacionados con la observancia de la ley. El nivel de flexibilidad concedido a tal efecto depende, una vez más, de la extensión de las medidas legislativas nacionales de aplicación de la Directiva de protección de datos en los sectores de policía y justicia, lo que puede limitar, totalmente o parcialmente, el derecho del interesado con el fin de asegurar el debido cumplimiento de las investigaciones y proteger la seguridad nacional.

187. Debe recordarse a este respecto que cualquier limitación de los derechos del interesado debe satisfacer con la CDFUE y el CEDH, tal como se interpreta en la jurisprudencia del TJUE y del TEDH, y principalmente respetar el contenido esencial de estos derechos y libertades.

188. Los Estados miembros deberán establecer obligaciones all responsable de datos para el tratamiento de datos personales. Desde el punto de vista de la seguridad de los datos y las obligaciones del responsable, observamos el nuevo planteamiento del legislador europeo en

[1674] Artículo 15 (Limitaciones al derecho de acceso) de la DIRECTIVA (UE) 2016/680. En este sentido, el Grupo de Trabajo había sugerido que se elimine de la propuesta la posibilidad de excluir categorías enteras de datos de estos derechos. ARTICLE 29 DATA PROTECTION WORKING PARTY (2013a: 3).
[1675] *Cfr*. *supra*, considerando 49 de la DIRECTIVA (UE) 2016/680.

esta materia que, en el RGPD, adoptó un enfoque completamente nuevo para la protección de datos personales. Se ha insistido varias veces en cómo el sistema ha pasado de ser un paradigma reactivo, a uno preventivo-precaucional, colocando el tratamiento y la correcta aplicación de sus principios con el máximo detalle posible, calibrando con precisión escrupulosa las obligaciones y responsabilidades de los principales actores del tratamiento y finalmente elaborando un sistema eficiente de medidas de seguridad que se conciba antes del tratamiento con el objetivo de reducir, si no eliminar por completo, el riesgo de lesiones graves a los derechos de los interesados. En particular, existe una obligación general para los responsables de implementar «*medidas técnicas y organizativas apropiadas*» para garantizar que el tratamiento se realice de acuerdo con la Directiva, y para poder demostrar la legalidad de dicho tratamiento[1676].

189. Las actividades del responsable deben cumplir con la nueva Directiva y el mismo debe implementar medidas que tengan en cuenta los principios de "protección de datos desde el diseño" y "protección de datos por defecto", y evaluar los fines del tratamiento, contexto, ámbito y naturaleza y «*los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas*»[1677]. En este contexto, las medidas de "protección de datos desde el diseño" y "por defecto" se introducen en el artículo 20: la protección de datos desde el diseño nombra explícitamente la seudonimización como posible medida técnica y organizativa pertinente; mientras que la protección de datos por defecto se refiere a medidas que aseguran que los datos personales por defecto no sean accesibles sin la intervención del individuo o de un número indefinido de individuos.

190. El principio de responsabilidad (en inglés, "*principle of accountability*") impone a los responsables de datos la carga de implementar por propia iniciativa medidas de protección de datos adecuadas en relación con el procesamiento que ejecutan. La evaluación de impacto de protección de datos se enumeran entre tales medidas: «*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales*»[1678]. El responsable del tratamiento debe

[1676] Artículo 19 de la DIRECTIVA (UE) 2016/680.
[1677] Considerandos 50, 52 y 53, artículos 19 y 20 de la DIRECTIVA (UE) 2016/680.
[1678] Artículo 27 (Evaluación de impacto relativa a la protección de datos) de la DIRECTIVA (UE) 2016/680. *Cfr*. artículo 32 del RGPD.

realizar una "evaluación de impacto sobre la protección de datos", que se centra, en particular, a las medidas, garantías y mecanismos previstos para garantizar la protección de los datos personales y para demostrar el cumplimiento de la Directiva. Aunque estos conceptos están inspirados en el RGPD, la Directiva aborda la naturaleza específica de las autoridades policiales y de justicia penal. En comparación con el tratamiento de datos para fines comerciales, que está regulado por el Reglamento, el tratamiento relacionado con la seguridad puede requerir cierto nivel de flexibilidad. Por ejemplo, proporcionar a los interesados el mismo nivel de protección en términos de derechos de información, acceso o eliminación de sus datos personales según el RGPD podría significar que cualquier operación de vigilancia llevada a cabo con fines policiales se volvería ineficaz en el contexto de la aplicación de la ley. Por lo tanto, en este sentido, la Directiva no contiene el principio de transparencia[1679].

191. El responsable del tratamiento debe evaluar los riesgos del tratamiento e implementar medidas para reducirlos, como el cifrado, para mantener la seguridad y evitar el tratamiento contrario a esta Directiva. En los casos en los que se haya producido una vulneración de datos personales, el responsable notifica a la autoridad de control, a menos que la vulneración no ponga en riesgo los derechos y las libertades de las personas físicas[1680].

192. Como es bien sabido, un elemento esencial del modelo de protección de datos es la creación de una (o varias) autoridad de control independiente encargada de supervisar la aplicación de la Directiva de protección de datos en cada Estado miembro[1681]. En este caso se han introducido normas similares a las existentes en el RGPD que se aplican para la cooperación con la autoridad de control y la definición de los casos en los que la consulta previa es obligatoria dentro de la autoridad (notificación de infracciones "*data breach*"[1682] e

[1679] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018).
[1680] Considerandos 60 y 61 de la DIRECTIVA (UE) 2016/680. Las personas deben ser informadas sin dilación indebida en caso de una violación de los datos personales que pueda presentar un "alto riesgo de sus derechos y libertades" para que puedan "adoptar las precauciones necesarias". «*La comunicación debe describir la naturaleza de la violación de los datos personales e incluir recomendaciones para la persona afectada*» a fin de mitigar los posibles efectos adversos. Considerando 62 y artículos 29 a 31 de la DIRECTIVA (UE) 2016/680.
[1681] Artículo 41 (Autoridad de control), apartado 1, de la DIRECTIVA (UE) 2016/680: «*Cada Estado miembro dispondrá que sea responsabilidad de una o varias autoridades públicas independientes supervisar la aplicación de la presente Directiva, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de sus datos personales y de facilitar la libre circulación de datos personales en la Unión*». *Cfr*. considerandos 75 a 77 de la DIRECTIVA (UE) 2016/680.
[1682] Artículo 48 (Notificación de infracciones) de la DIRECTIVA (UE) 2016/680: «*Los Estados miembros dispondrán que las autoridades competentes establezcan mecanismos eficaces que fomenten la notificación confidencial de infracciones a la presente Directiva*».

informe de actividad[1683]). Las competencias, funciones y poderes (limitados) de las autoridades de control[1684] recuerdan el régimen reconocido por el Reglamento[1685], así como la división tripartita de poderes de investigación[1686], correctivos y consultivos efectivos[1687], pero en la Directiva de 2016 la referencia a las actividades a desarrollar es mucho más lacónica, dejando, de nuevo, espacio al legislador nacional. Por ejemplo, en este sentido, la autoridad de control establecida a los efectos de la Directiva puede ser la misma que la autoridad de control establecida en virtud del RGPD, pero los Estados miembros son libres de designar una autoridad diferente, siempre que cumpla los criterios de independencia[1688].

193. Para garantizar un control eficaz, fiable y coherente del cumplimiento y la ejecución de la Directiva en toda la Unión, de conformidad con el TFUE según ha sido interpretado por el TJUE, las autoridades de control deben tener las mismas funciones y poderes en cada Estado miembro, incluidos los poderes de investigación, corrección y asesoramiento, que constituyen los medios necesarios para llevar a cabo sus funciones. Sin embargo, "sus poderes no deben interferir con las normas específicas para los procesos penales, incluida la investigación y el enjuiciamiento de los delitos". Los poderes de las autoridades de control se ejercerán de conformidad con las «*garantías procesales adecuadas establecidas*» por el Derecho de la Unión y la legislación del Estado miembro, de «*forma imparcial y justa*» y

[1683] Artículo 49 (Informe de actividad) de la DIRECTIVA (UE) 2016/680: «*Cada autoridad de control elaborará un informe anual sobre sus actividades, que podrá incluir una lista de los tipos de infracciones notificadas y de tipos de las sanciones impuestas. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho del Estado miembro. Se pondrán a disposición del público, de la Comisión y del Comité Europeo de Protección de Datos*».

[1684] Considerandos 81 a 83, artículos 45 a 47 (Capítulo VI, Autoridades de control independientes - Sección 2, Competencia, funciones y poderes) de la DIRECTIVA (UE) 2016/680. Cada autoridad de supervisión debe tratar las quejas presentadas por cualquier parte interesada y llevar a cabo las investigaciones relacionadas o remitirlas a la autoridad de supervisión competente. Después de una queja, se debe realizar una investigación, sujeta a revisión judicial, en la medida en que sea apropiada en este caso. La autoridad de control debe informar a los interesados sobre el estado y el resultado de la queja dentro de un tiempo razonable. «*Si el caso requiere mayor investigación o coordinación con otra autoridad de control*», el interesado debe recibir intermediario interlocutor (considerando 81). En un informe el Grupo de Trabajo había recomendado ampliar el artículo 46 de la propuesta de Directiva del Parlamento Europeo y del Consejo sobre los poderes de las autoridades de supervisión y añadir la posibilidad de acceder a todos los documentos necesarios para el ejercicio de sus investigaciones. Según el Grupo, esta modificación ofrecería una supervisión completa en el tratamiento de datos dentro del ámbito policial y judicial, equivalente a la que encontramos actualmente en la Directiva 95/46/CE. ARTICLE 29 DATA PROTECTION WORKING PARTY (2013a: 7).

[1685] *Cfr*. artículo 58 del REGLAMENTO (UE) 2016/679.

[1686] Artículo 47, apartado 1, de la DIRECTIVA (UE) 2016/680.

[1687] Artículo 47, apartados 2 y 3, de la DIRECTIVA (UE) 2016/680.

[1688] Los Estados miembros ya han establecido la autoridad de supervisión en virtud del RGPD y las funciones en virtud de la nueva Directiva pueden transferirse a esta autoridad. Artículo 41, apartado 3, de la DIRECTIVA (UE) 2016/680: «*Los Estados miembros podrán disponer que una autoridad de control creada en virtud del Reglamento (UE) 2016/679 pueda ser la autoridad de control mencionada en la presente Directiva y asuma la responsabilidad de las funciones de la autoridad de control que vayan a crearse de conformidad con el apartado 1 del presente artículo*».

dentro de «*un plazo razonable*». En particular, cada medida debería «*ser adecuada, necesaria y proporcionada*» para garantizar el cumplimiento de la Directiva[1689].

194. «*Los Estados miembros dispondrán que sus autoridades de control se faciliten entre sí información útil y se presten asistencia mutua*»[1690], tomando medidas[1691] para asegurar una efectiva cooperación entre ellas[1692]. La cooperación de las autoridades de control se lleva a cabo a través del Comité Europeo de Protección de Datos establecido por el Reglamento[1693], en el que participan las autoridades designadas por el legislador nacional para supervisar la aplicación de los procesamientos de datos en los sectores incluidos en la Directiva (UE) 2016/680.

4.4. Transferencias de datos personales a terceros países u organizaciones internacionales: la falta de cooperación en el intercambio de información

195. Las autoridades públicas del Estado miembro de la UE pueden transferir información a las autoridades públicas de otros Estados en relación con su trabajo. Hasta ahora, esto había sido regulado por el Convenio n. 108, guiado por la Recomendación R (87) 15 sobre datos policiales del Consejo de Europa y la Decisión Marco 2008/977/JAI del Consejo[1694]. La Directiva de protección de datos en materia de policía establece que la

[1689] Considerando 82. Los Estados miembros deben implementar e "imponer sanciones", que sean "efectivas", "proporcionadas y disuasorias", para las personas que incumplan la Directiva. Si el interesado considera que se han violado sus derechos en virtud de la Directiva o si la autoridad de control no actúa sobre su reclamación, «*tiene derecho a un recurso judicial efectivo de conformidad con el artículo 47 de la Carta*» (considerando 85). «*Toda persona física o jurídica debe tener derecho a un recurso judicial*» efectivo ante los tribunales nacionales competentes contra una decisión de la autoridad de control que produzca efectos jurídicos con respecto a esa persona (considerando 86). También *vid*. artículo 47, apartados 4 y 5, de la DIRECTIVA (UE) 2016/680.

[1690] Artículo 50 (Asistencia mutua) de la DIRECTIVA (UE) 2016/680.

[1691] También se insertó una disposición que exige al legislador nacional establecer que las autoridades competentes pongan en obra «*mecanismos eficaces que fomenten la notificación confidencial de infracciones a la presente Directiva*». Artículo 48 (Notificación de infracciones) de la DIRECTIVA (UE) 2016/680.

[1692] «*La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo consultas, inspecciones e investigaciones*». Cada autoridad de control adoptará «*todas las medidas apropiadas requeridas para responder a la solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes tras haber recibido la solicitud*». Artículo 50 de la DIRECTIVA (UE) 2016/680.

[1693] Artículo 51 (Funciones del Comité Europeo de Protección de Datos) de la DIRECTIVA (UE) 2016/680. El Comité sustituye el Grupo de Trabajo "Artículo 29" creado por la Directiva 95/46/CE. En lo que se refiere a la Directiva de protección de datos en los sectores de policía y justicia, parece sólo un aparente reemplazo, ya que tendrá esencialmente los mismos poderes del Grupo de Trabajo.

[1694] A este respecto, cabe destacar que el tratamiento de datos en el contexto de policía y justicia penal era un campo que quedaba, hasta ahora, fuera de la legislación de la Unión Europea; es por eso que prácticamente todos los Estados miembros tienen acuerdos bilaterales con terceros países que permiten el intercambio de datos personales con fines relacionados con la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, a pesar de cualquier nivel de adecuación en el respeto de las garantías de protección de datos de los destinatarios.

autoridad competente de un Estado miembro puede enviar datos personales a la autoridad competente de un tercer país, si la transferencia cumple con las condiciones de la Directiva.

196. De forma similar al RGPD, la Directiva establece los requisitos para la transferencia de datos personales a terceros países u organizaciones internacionales. Si los datos personales se transmitieran libremente fuera de la jurisdicción de la UE, se podrían socavar las salvaguardas y la protección sólida que ofrece la legislación de la UE. Sin embargo, las condiciones en sí mismas son bastante diferentes a las del RGPD[1695].

197. Como sabemos, a fin de intercambiar información pertinente para que puedan realizar las funciones que les determina la ley, las autoridades competentes de los Estados miembros aplican acuerdos internacionales bilaterales o multilaterales existentes celebrados con terceros países en el ámbito de la cooperación judicial en materia penal y cooperación con la policía. Esto se hace mediante la cooperación de las autoridades competentes de los terceros países a los efectos de la Directiva, a veces incluso a falta de un acuerdo bilateral o multilateral internacional. Por tanto, con respecto a las «*transferencias de datos personales a terceros países u organizaciones internacionales*», la Directiva, en el artículo 35 y ss., contempla diferentes circunstancias para transferir datos desde un Estado de la Unión a un tercer Estado u organismo internacional, expresando así que "se quiere privilegiar una eficaz cooperación policial en este tipo de tratamiento". La transferencia de datos personales a terceros países o internacionales puede realizarse solamente cuando se hayan cumplido las siguientes condiciones: 1) la transferencia es necesaria para los fines de la Directiva; 2) los datos personales se transfieren a una autoridad competente, en el sentido de la Directiva, del tercer país o de la organización internacional, aunque existe una excepción a esta regla en casos particulares y específicos (en este sentido, *vid. infra* artículo 39); 3) cuando los datos personales se «*transmitan o procedan de otro Estado miembro*», y dicho Estado miembro haya proporcionado su «*autorización previa para la transferencia de conformidad*» con su legislación nacional; 4) la Comisión Europea ha adoptado «*una decisión de adecuación*», se han establecido "garantías apropiadas" o se aplica la "excepción para transferencias en

[1695] Diferencias que se deducen del propio RGPD 2016/679, artículo 44 (Principio general de las transferencias) al determinar: «*Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado*».

situaciones específicas"; 5) las "transferencias ulteriores" de datos personales a otro tercer país o a una organización internacional requieren la autorización previa de la autoridad competente de origen, que tendrá en cuenta, entre otras cosas, la gravedad del delito y «*el nivel de protección de datos personales en el tercer país u organización internacional a los que se transfieran ulteriormente los datos personales*»[1696].

198. El punto de partida de nuestro discurso es que la norma europea que se examina dispone que la transferencia sea precedida por una decisión de adecuación de la Comisión[1697] sobre el nivel de protección de datos en el país que debería recibirlos. En base a eso, una transferencia de datos personales a un tercer país o una organización internacional «*pueda realizarse* (…) *cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado*[1698]. *Dicha transferencia no requerirá ninguna autorización específica*»[1699]. Sin embargo, los Estados miembros podrán prever que la transferencia se lleve a cabo sin autorización previa del Estado del que provienen los datos si tienen el propósito de «*prevenir una amenaza inmediata y grave para la seguridad pública de un Estado miembro, o de un tercer país, o para los intereses fundamentales de un Estado miembro*», y si el responsable del tratamiento en el tercer país u organización internacional en cuestión «*es una autoridad competente*»[1700]. Sólo las autoridades competentes que actúen como responsables del tratamiento deben llevar a cabo las transferencias.

199. El primer requisito, establecido por el artículo 36, apartado 2, al evaluar la adecuación del nivel de protección, la Comisión tiene en cuenta, en particular, los siguientes elementos: «*a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluidas la seguridad pública, la defensa, la seguridad nacional, el Derecho penal y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de los datos,* (…) *incluidas las normas para las transferencias*

[1696] Artículo 35 (Principios generales de las transferencias de datos personales), apartado 1, de la DIRECTIVA (UE) 2016/680.
[1697] Artículo 36 (Transferencias basadas en una decisión de adecuación) de la Directiva (UE) 2016/680.
[1698] Como ya conocimos, el concepto de "nivel adecuado" de protección ha sido definido por el TJUE en el caso *Schrems*, nos referimos en particular al apartado 73 de la sentencia (*vid*. *supra*). Obliga al tercer país, de hecho, a garantizar, en virtud de su legislación interna o de sus compromisos internacionales, un nivel de protección de los derechos y libertades fundamentales que son esencialmente equivalentes a los protegidos dentro de la Unión Europea.
[1699] Artículo 36, apartado 1, de la DIRECTIVA (UE) 2016/680. *Cfr*. artículo 25 (Transferencia de datos personales a países terceros y organizaciones internacionales) del Reglamento Europol.
[1700] Artículo 35, apartado 2 y *cfr*. con el considerando 64 y de la DIRECTIVA (UE) 2016/680.

ulteriores de datos personales a otro tercer país u organización internacional que se apliquen en el tercer país o en la organización internacional en cuestión, la jurisprudencia, así como los derechos del interesado efectivos y exigibles y un derecho de recurso administrativo y judicial efectivo de los interesados cuyos datos personales son transferidos»[1701]. El segundo requisito al evaluar la adecuación del nivel de protección, es que la Comisión tendrá en cuenta «*b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y ejecutar el cumplimiento de las normas en materia de protección de datos, incluidos los poderes ejecutivos adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros*»[1702].

200. La «*adopción de una decisión de adecuación*» con respecto a «*un territorio o sector específico*» dentro de un tercer país debe «*tener en cuenta criterios y objetivos*» claros, como las actividades específicas de procesamiento y el alcance de aplicación de las normas y de la legislación aplicable vigente en el tercer país. El tercer país «*debe ofrecer garantías*» para garantizar un nivel adecuado «*de protección esencialmente equivalente al garantizado*» dentro de la UE, en particular cuando los datos se tratan en uno o más sectores específicos. En particular, el tercer país debería «*garantizar*» un "control independiente efectivo" de la protección de datos y debe prever «*mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros*», y consentir a las partes interesadas «*derechos efectivos y exigibles*», así como un recurso efectivo en sede administrativa y judicial[1703]. Como consecuencia de lo dicho, esta norma se basa en los valores fundamentales en los que se fundamenta la UE, en particular *in primis* la protección de los derechos humanos y libertades fundamentales. Por lo tanto, la Comisión debe considerar hasta qué punto en ese tercer país se «*respeta el Estado de Derecho, el acceso a la justicia,* (…) *la seguridad pública, la defensa y la seguridad nacional, así como el Derecho penal y el orden público*»[1704].

201. Por último, la Comisión tendrá en cuenta, al evaluar la adecuación del nivel de protección, «*c) los compromisos internacionales asumidos por el tercer país o la organización internacional correspondiente, u otras obligaciones que deriven de convenios*

[1701] Artículo 36, apartado 2, letra a), de la DIRECTIVA (UE) 2016/680.
[1702] Artículo 36, apartado 2, letra b), de la DIRECTIVA (UE) 2016/680.
[1703] Considerando 67 de la DIRECTIVA (UE) 2016/680.
[1704] Considerando 67 de la DIRECTIVA (UE) 2016/680.

o instrumentos jurídicamente vinculantes o de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales»[1705]. La Comisión, en el tercer elemento, «*debe tener en cuenta las obligaciones*» derivadas de la «*participación del tercer país*» o de la organización internacional en sistemas multilaterales o regionales, especialmente «*en relación con la protección de datos personales*», así como la implementación de estas obligaciones". En particular, la Comisión debe tener «*en cuenta la adhesión*» de terceros países al Convenio n. 108 y su Protocolo adicional. Al evaluar la idoneidad del nivel de protección en terceros países u organizaciones internacionales, la Comisión debe consultar al Comité Europeo de Protección de Datos establecido por el RGPD[1706]. La Comisión también debe tener en cuenta las decisiones de adecuación pertinentes adoptadas de conformidad con el artículo 45 del mismo Reglamento[1707].

202. Analizados los requisitos descritos previamente, la Comisión decidirá, con un "acto de ejecución", dentro del «*ámbito de aplicación*» de la Directiva, si un tercer país, un territorio o uno o más sectores específicos dentro de un tercer país, o una organización internacional garantizan un nivel adecuado de protección[1708].

203. En cambio, en el caso que la Comisión decida que un tercer país, o uno o más sectores específicos en ese tercer país, o una organización internacional «*han dejado de garantizar un nivel de protección adecuado*», según los requisitos anteriormente determinados en el apartado 2, podrá «*derogar, modificar o suspender la decisión,* (…) *mediante actos de ejecución, sin efecto retroactivo*»[1709]. En consecuencia, «*debe prohibirse la transferencia de datos personales*» a este tercer país u organización internacional, a menos que «*se cumplan los requisitos*» de la Directiva con respecto a las transferencias sujetas a las garantías adecuadas y las excepciones para situaciones específicas[1710]. En este caso los

[1705] Artículo 36, apartado 2, letra c), de la DIRECTIVA (UE) 2016/680.
[1706] Considerando 68 de la DIRECTIVA (UE) 2016/680.
[1707] Sobre el artículo 45 del RGPD, *vid*. *supra*.
[1708] El artículo 36, apartado 3, de la DIRECTIVA (UE) 2016/680 reconoce que la Comisión, «*tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado*» a tenor de las obligaciones dispuestas en el apartado 2 del presente artículo. El mismo artículo aclara que «*el acto de ejecución contendrá un mecanismo para su revisión periódica, como mínimo cada cuatro años, que tendrá en cuenta todos los acontecimientos que sean de interés en el tercer país u organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial y, cuando proceda, determinará cuál es la autoridad o autoridades de control a que se refiere* (…)».
[1709] Artículo 36, apartado 5, de la DIRECTIVA (UE) 2016/680.
[1710] Considerando 70 de la DIRECTIVA (UE) 2016/680. «*La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de los terceros países, territorios y sectores específicos en un*

Estados miembros dispondrán que pueda producirse una transferencia de datos personales a un tercer país o una organización internacional cuando: «*a) se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante, o b) el responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales*»[1711].

204. También, se establecen excepciones para situaciones específicas en las que, los Estados miembros, en «*ausencia de una decisión de adecuación de conformidad*», o de garantías apropiadas de conformidad, se asegurarán de que una transferencia o una categoría de transferencias de datos personales a un tercer país o una organización internacional solo pueda realizarse a condición de que la transferencia sea necesaria: «*a) para proteger los intereses vitales del interesado o de otra persona; b) para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales; c) para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país; d) en casos individuales a efectos del artículo 1, apartado 1* (es decir, prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública); *e) en un caso individual para el establecimiento, el ejercicio o la defensa de acciones legales en relación con los fines expuestos en el artículo 1, apartado 1*»[1712]. Las excepciones deben interpretarse de "forma restrictiva" y no deben permitir transferencias frecuentes, en masas y estructurales de datos personales o transferencias de datos "a gran escala", sino deben "limitarse a los datos estrictamente necesarios". Dichas transferencias deben documentarse y, previa solicitud,

tercer país, y de las organizaciones internacionales para los que haya decidido que sigue o no garantizado un nivel de protección adecuado». Artículo 36, apartado 8, de la DIRECTIVA (UE) 2016/680.

[1711] Artículo 37 (Transferencias mediante garantías apropiadas), apartado 1, de la DIRECTIVA (UE) 2016/680. Dichos «*instrumentos jurídicamente vinculantes*» podrían consistir, por ejemplo, en «*acuerdos bilaterales jurídicamente vinculantes*» que hayan sido «*celebrados por los Estados miembros*» e incorporados en su ordenamiento jurídico y que puedan ser invocados por sus interesados, a fin de garantizar el cumplimiento de «*los requisitos de protección de datos y derechos de los interesados*», incluido el derecho a una «*tutela efectiva*» en procedimientos administrativos o judiciales. Al evaluar «*todas las circunstancias de la transferencia de datos*», el responsable del tratamiento debe poder «*tener en cuenta los acuerdos de cooperación celebrados entre Europol o Eurojust y terceros países que permitan el intercambio de datos personales*». El «*responsable del tratamiento*» de datos también debe tener en cuenta que la transferencia de datos personales estará sujeta a «*obligaciones de confidencialidad y al principio de especificidad*», a fin de garantizar que los datos no se traten «*para fines distintos de aquellos para los que se han transferido*». Considerando 71 de la DIRECTIVA (UE) 2016/680.

[1712] Artículo 38 (Excepciones para situaciones específicas), apartado 1, de la DIRECTIVA (UE) 2016/680.

ponerse a disposición de la autoridad supervisora para permitir el control de la licitud de las transferencias[1713].

205. Sin embargo, en «*casos particulares y específicos*», a pesar del artículo 35, apartado 1, letra b), y «*sin perjuicio de todo acuerdo internacional*», el Derecho de la Unión o del Estado miembro podrá disponer que las autoridades competentes permitan la transferencia de datos personales de las autoridades competentes a destinatarios establecidos en terceros países si, además de cumplir una de las tres condiciones descritas anteriormente, satisfacen también todas las siguientes condiciones adicionales establecidas en el artículo 39 de la Directiva. En particular, la transferencia debe ser «*estrictamente necesaria para la realización de una función de la autoridad competente de la transferencia*», que también es responsable de determinar que ningún derecho o libertad fundamental de los individuos prevalece sobre el interés público que justifica la transferencia. Además, la autoridad competente que opera la transferencia considerará que la transferencia a una autoridad competente del tercer país sea «*ineficaz o inadecuada*», en particular no se puede llevar a cabo con prontitud[1714].

206. Con el objetivo de este artículo se puede entender que, en casos específicos individuales, los procedimientos normales que requieren contactar a «*la autoridad del tercer país pueden ser ineficaces o inadecuados*», en particular porque la transferencia no pudo llevarse a cabo oportunamente, o porque esa autoridad en el tercer país no respeta el Estado de Derecho o las normas y estándares internacionales de derechos humanos, de modo que «*las autoridades competentes de los Estados miembros*» puedan «*decidir transferir los datos personales directamente*» a los destinatarios establecidos en esos terceros países. Esto podría ocurrir si hay «*una necesidad urgente de transferir datos personales para salvar la vida de una persona que esté en peligro de ser víctima de una infracción penal*» o para evitar «*la comisión inminente de un delito*», incluido el terrorismo[1715]. Finalmente, podemos concluir que, entre las situaciones examinadas, está la posibilidad de transferir dichos datos a un tercer país que no garantice un nivel adecuado de protección.

207. En efecto, aquí de nuevo la Directiva tenía que mantener un cuidadoso equilibrio entre, por una parte, las exigencias policiales y de justicia criminal y de los acuerdos

[1713] Considerando 72 de la DIRECTIVA (UE) 2016/680.
[1714] Artículo 39 (Transferencias de datos personales a destinatarios establecidos en terceros países), apartado 1, letra c), de la DIRECTIVA (UE) 2016/680.
[1715] Considerando 73 de la DIRECTIVA (UE) 2016/680.

bilaterales existentes y, por otro, la exigencia de un nivel de protección de datos personales más alto. Por ejemplo, la misma norma en examen no dice mucho sobre los acuerdos bilaterales ya existentes[1716]. Ciertamente, los acuerdos bilaterales vigentes entre los Estados de la UE y terceros países permanecen así hasta que no se cambie. Es cierto que este texto afecta a todos los acuerdos bilaterales, que necesitan modificaciones para que se armonicen con las normas de la Directiva. Sin embargo, si los Estados miembros, que no tienen la obligación de modificar los acuerdos bilaterales, no toman medidas, la existencia prolongada de los acuerdos bilaterales que se aplican a los estándares más bajos reconocidos en la Directiva podrían socavar todo el conjunto de la transferencia internacional de datos.

208. La transferencia transfronteriza de datos personales, pueden poner en peligro la posibilidad de las personas físicas de «*ejercer sus derechos de protección de datos*», frente a la utilización ilícita, y las autoridades de control pueden ser incapaces de operar fuera de sus fronteras. Esto nos lleva a la existencia de un serio problema de no compartir, de manera satisfactoria, la información personal[1717] entre los Estados miembros, lo que contradice la *ratio* de las bases de datos y obstacula la cooperación internacional. Por tanto, «*es necesario fomentar una cooperación más estrecha entre las autoridades de control de protección de datos para ayudarles a intercambiar información con sus homólogos extranjeros*»[1718]. Por esta razón, la cooperación entre las autoridades de control necesita desarrollo para ayudarlos a intercambiar información[1719] con sus contrapartes extranjeras. La Directiva de protección de datos sobre asuntos policiales también lo reconoce.

209. Dentro de la misma línea, para la protección de los datos personales, la Directiva establece claramente "mecanismos de cooperación internacional", en relación con terceros países y organizaciones internacionales, la Comisión y los Estados miembros adoptan

[1716] Artículo 39, apartado 2, DIRECTIVA (UE) 2016/680: «*Por acuerdo internacional mencionado en el apartado 1 se entenderá todo acuerdo internacional bilateral o multinacional en vigor entre los Estados miembros y terceros países en el ámbito de la cooperación judicial en asuntos penales y de la cooperación policial*».

[1717] Según el considerando 21 de la DIRECTIVA (UE) 2016/680 «*Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Para determinar si una persona física es identificable deben tenerse en cuenta todos los medios con respecto a los cuales existe una probabilidad razonable de que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona para la identificación directa o indirecta de dicha persona física*».

[1718] Considerando 74 de la DIRECTIVA (UE) 2016/680.

[1719] Esta falta de compartir información es «*el principal problema ante los ataques terroristas y otros crímenes trasnacionales es que los cuerpos judiciales y de seguridad son reacios a compartir información valiosa*», explicó la ponente de la Directiva, Marju Lauristin (S&D, Estonia). También la misma añadió, «*al fijar estándares europeos para el intercambio de información, esta norma se convertirá en una herramienta útil para ayudar a las autoridades a trasladar datos personales de manera sencilla y efectiva, asegurando el respeto al derecho fundamental a la privacidad*». En PARLAMENTO EUROPEO - Notas de prensa (2016b).

«*medidas apropiadas*» para: «*a) crear mecanismos de cooperación internacional que faciliten la aplicación efectiva de la legislación relativa a la protección de datos personales; b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales; c) procurar la participación de las correspondientes partes interesadas en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales; d) promover el intercambio y la documentación de la legislación y prácticas en materia de protección de datos personales, inclusive en los conflictos jurisdiccionales con terceros países*»[1720].

210. En relación con el intercambio de datos de la UE a terceros países, la función principal de la Comisión de la UE es garantizar que se reconozcan los principios de protección de datos. La Comisión decide para toda la UE si los terceros países y las organizaciones internacionales proporcionan un nivel adecuado de protección. Esto es para lograr la uniformidad y la seguridad jurídica en toda la UE. La definición de adecuación de la protección se deriva, como ya se haampliamente debatido, de la interpretación del TJUE en el caso *Schrems* y, a partir de ahí, se escribe en los considerandos de esta Directiva[1721]. Además, el nivel de protección en un tercer país es adecuado cuando es esencialmente equivalente al de la UE. Pero, el estándar "esencialmente equivalente" es difícil de cumplir en el campo de la ley de seguridad nacional[1722].

[1720] Artículo 40 (Cooperación internacional en el ámbito de la protección de datos personales) de la DIRECTIVA (UE) 2016/680.

[1721] En particular en el considerando 67 de la Directiva (UE) 2016/680: «*En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación de un tercer país, de un territorio, o de un sector específico de un tercer país, debe tener en cuenta la medida en que dicho tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y principios internacionales en materia de derechos humanos, y su Derecho tanto general como sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el Derecho penal y el orden público. En la adopción de una decisión de adecuación en relación con un territorio o un sector específico de un tercer país, se deben tener en cuenta criterios claros y objetivos, como las actividades de tratamiento concretas y el ámbito de aplicación de las normas jurídicas y la legislación vigentes en el tercer país. El tercer país en cuestión debe ofrecer garantías que aseguren un nivel de protección adecuado que sea esencialmente equivalente al garantizado en el interior de la Unión, en particular cuando los datos se sometan a tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar la supervisión eficaz e independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, y ofrecer a los interesados derechos efectivos y exigibles, así como un derecho a la tutela administrativa y judicial efectiva*».

[1722] Quien entre en posesión de una información útil sobre la seguridad pública, en seguida la comunicará inmediatamente a los demás Estados miembros; pero eso se hace sólo en raras ocasiones. Significativo de esta tendencia de los estados europeos es una declaración de la Alta Representante de la Unión

211. Por lo tanto, el punto crucial es siempre la misma cuestión: la dificultad de encontrar el equilibrio adecuado entre las medidas eficaces y la protección de datos personales de los ciudadanos europeos. Algunos de los principales recursos citados antes con los que la Unión Europea, a través la Directiva, tratan de poner de acuerdo a las autoridades judiciales y policiales de diferentes países, y, sobre todo, dar un impulso particular a la cooperación con las autoridades nacionales antes de facilitar cada tratamiento, a partir del cual la privacidad de los ciudadanos europeos puede salir perjudicada, porque aún seguirá habiendo diversos sistemas de información europeos que quedarán fuera del alcance de ese instrumento legislativo, lo cual significa que no se conseguirá una armonización de las normas de protección de datos en el ámbito policial y judicial.

4.5. ¿La Directiva de protección de datos en los sectores policial y judicial protege nuestra privacidad?

212. El espíritu de la Directiva (UE) 2016/680, se podría resumir en su objetivo de respetar el derecho a la privacidad para garantizar una mejor y más eficaz seguridad de los ciudadanos europeos. Por consiguiente, más privacidad y más seguridad al mismo tiempo, ya que no tiene que renunciar a la primera para garantizar la segunda. Un espíritu que parece ser la mejor respuesta posible a los muchos que, en los últimos años, a raíz de la amenaza terrorista, parecieron convencidos de que la privacidad tuviera que dar paso a la seguridad y que para realizar esto fuera necesario renunciar a la primera. En todo caso, la tarea pasa a los parlamentos y gobiernos nacionales que tendrán que transponer correctamente y sin demora el contenido de la Directiva. Sin embargo, el proceso de implementación está en sus comienzos, por lo que resulta difícil decir cómo van a cambiar las legislaciones nacionales.

---

para Asuntos Exteriores y Política de Seguridad, Federica Mogherini, que, durante un Consejo de Asuntos Exteriores (CAE), donde se discutió diferentes posibles líneas de acción respecto a la lucha contra el terrorismo, y reuniendo un consenso para fortalecer el intercambio de información entre los países miembros y una mayor cooperación con los países árabes y mediterráneos, afirmó que «*Por primera vez, existe un verdadero convencimiento de que es necesario trabajar juntos en la lucha contra el terrorismo* (…) *para cooperar de una manera mucho más activa de lo que se había hecho hasta la fecha*». Pero este optimismo tiene que lidiar con el hecho de que el intercambio de información de inteligencia entre Estados miembros siempre ha sido un obstáculo para la plena cooperación en varias áreas de preocupación de la seguridad. No parece, por lo tanto, aún una actitud suficientemente extendida en Europa a las formas de cooperación de información eficaz y, mucho menos, la Directiva en examen resuelve el problema. El Consejo se había reunido unos pocos días después del ataque terrorista en París. CONSEJO EUROPEO (2015), Consejo de Asuntos Exteriores, 19.1.2015, Sesión n. 3364, Bruselas, 19.1.2015. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/fac/2015/01/19/. También tenemos que registrar que los actos de las autoridades europeas tampoco son siempre transparentes. Por ejemplo, el año pasado salió a la luz que los servicios secretos alemanes recopilaban datos y espiaban excesivamente a los socios de la UE presuntamente desde 1999. *Vid*. «Los servicios secretos alemanes espiaron a medios extranjeros, según 'Der Spiegel'», en *El Confidencial*, 24.02.2017. Disponible en Internet: https://www.elconfidencial.com/mundo/2017-02-24/servicios-secretos-alemania-espiarion-medios-extranjeros-spiegel_1338357/ [documentos consultados: 01 de julio de 2017].

De todos modos, no parecen suficientes las disposiciones europeas para llegar a un punto de armonía entre las demandas de seguridad colectiva y derechos individuales a la luz de las modificaciones continuas que experimentan en función de las inquietudes planteadas en los ciudadanos.

213. Nos enfrentamos a posibles ventajas y problemas de la legislación uniforme de protección de datos en materia policial en la UE. La uniformidad asegura la misma protección y mejora la cooperación entre las autoridades, pero la nueva Directiva abstracta permite a los Estados miembros adoptar legislaciones nacionales que difieren significativamente entre sí.

214. En un primer balance, parece que no hay novedades de relieve en los sesenta y cinco artículos y 107 considerandos a lo largo de los cuales se desarrolla la Directiva. Sólo la reafirmación puntual de los principios, algunos de ellos ya reconocidos en el RGPD, y también en la Decisión Marco 2008/977/JAI del Consejo, que inspiran la normativa europea sobre la privacidad y sólo una inequívoca afirmación que, a tal principio, en todos los países europeos, se aplicarán también a las autoridades judiciales y de policía[1723]. Sin embargo, se muestra una especial preocupación con respecto a la eficacia de la aplicación de las normas en la práctica, especialmente cuando la legislación nacional no separa la seguridad nacional y la función policial (como el caso de la legislación de Reino Unido e Irlanda), acentuando aún más las diferencias entre los 28 Estados miembros de la UE[1724]. En consecuencia, se debe evitar cada posible confusión entre las competencias de las agencias de información y las de la policía judicial[1725].

[1723] Antes de la entrada en vigor de la Directiva (UE) 2016/680, mayo de 2018, los Estados miembros de la UE tenían la posibilidad de interpretar de forma independiente los principios de protección de los datos personales tratados en el marco de la cooperación policial en materia penal según lo establecido en el Convenio n. 108. Cuando las autoridades nacionales transmiten datos personales a las autoridades de otros Estados, está cubierto por la Decisión marco del Consejo 2008/977/JAI si ese Estado miembro ha aplicado la Decisión en su legislación nacional.

[1724] Un ejemplo concreto de las diferencias entre la legislación de los Estados miembros se puede encontrar en el caso *S. and Marper contra Reino Unido*, sentencia de 4 de diciembre de 2008 emitida por el TEDH que mostró los diferentes enfoques de los Estados miembros sobre la toma obligatoria de información de ADN en el contexto de un proceso penal. En algunos países, se limitaba a circunstancias específicas, sin embargo, en el Reino Unido, era una retención sistemática e indefinida, independientemente de la presunta ofensa o la edad del delincuente. TEDH, *S. and Marper contra Reino Unido*, apartados 45-47.

[1725] También son muy importantes, a los presentes efectos, tres sentencias, respectivamente, de los tribunales constitucionales alemán y portugués. La sentencia n. 31/2013 del Tribunal Constitucional de Alemania, en la que se anula parcialmente la ley sobre la recopilación y el intercambio de datos con fines de lucha contra el terrorismo. El Tribunal, en particular, reafirmó el principio de la separación de la información recogida con fines de inteligencia de los utilizados para el propósito de policía y la necesidad requerida de carácter obligatorio de los presupuestos legitimadores de los poderes de adquisición de datos personales por las agencias, señalando sin embargo que, en vista de la extensión de los poderes, es aún más necesario una supervisión adecuada por parte de las autoridades de protección de datos. La sentencia de 20 de abril de 2016,

215. Así que, por una parte, estamos asistiendo a medidas destinadas a reafirmar la necesidad de proteger el derecho a la protección de los datos personales de los individuos y, por otro lado, hay que hacer frente a las diferentes legislaciones nacionales, debido a un equilibrio diferente entre razones de seguridad, que empujan cada vez un procesamiento de datos siempre más amplio, y las garantías individuales. En consecuencia, la investigación policial será complicada cuando involucre a varias jurisdicciones ya que la legislación no está armonizada. En tanto los Estados miembros pueden adoptar una legislación que implemente las disposiciones de la Directiva de manera diferente que otros Estados, esto puede crear efectos negativos para los interesados y un trato desigual entre los Estados miembros. Los diferentes modelos de protección de datos complicarán el intercambio de información y obstaculizarán la cooperación entre las autoridades. Es difícil identificar a las personas involucradas en el crimen, la jurisdicción competente y obtener evidencia.

216. Consecuencia de lo dicho, es cierto que deberían introducirse disposiciones que sometan a esas autoridades nacionales que están involucradas en actividades de recopilación de datos a normas uniformes, por lo que, una vez más, pueden facilitar una confianza mutua (condición previa para una cooperación eficaz), pero, sobre todo, para evitar la creación de zonas grises, peligrosas para la protección de los derechos de los individuos objeto de tratamiento de datos por fines de seguridad. Este es el caso, por ejemplo, de las técnicas y tecnologías de vigilancia sobre los movimientos y transacciones de personas, bienes de propiedad o utilizados por ellos con el fin de dar lugar a la creación de bases de datos adicionales que pueden utilizarse para la "guerra contra el terror"[1726].

---

emitida por el mismo Tribunal Constitucional alemán, ha vuelto a abordar el tema de los límites de investigaciones realizadas con instrumentos de vigilancia oculta y, en particular, el uso de los instrumentos de vigilancia computarizados que permiten la adquisición de datos remotos. La decisión del Tribunal Constitucional portugués de 27 de agosto de 2015 declaró nulo el poder de acceso a los servicios secretos a los tabulados de los equipos móviles, proporcionado por la legislación antiterrorista. El Tribunal Constitucional consideró que la adquisición de estos datos, en ausencia de autorización judicial, similar a la del proceso penal, constituye una injerencia particularmente grave en las comunicaciones privadas, donde se garantiza su privacidad por la Ley Fundamental. *Vid*. Counter-terrorism database in its fundamental structures compatible with the Basic Law, but not regarding specific aspects of its design, Press Release N. 31/2013 of 24 April 2013. Sobre una reconstrucción minuciosa judicial y normativa, así como un análisis exhaustivo del caso tratado y el resultado de la sentencia de 2016, véase Annalisa REGI (2016), «La Corte Costituzionale tedesca affronta il tema dei limiti alle investigazioni compiute con strumenti di sorveglianza occulta: come contemperare il dovere dello Stato di proteggere la popolazione dalle gravi forme di criminalità con la garanzia dei diritti fondamentali della persona?», en *filodiritto.com*, 22 giugno 2016. Disponible en Internet: http://www.filodiritto.com/articoli/2016/06/la-corte-costituzionale-tedesca-affronta-il-tema-dei-limiti-alle-investigazioni-compiute-con-strumenti-di-sorveglianza.html. Por último, Tribunal Constitucional chumba acceso das secretas a dados bancários e de comunicações, Disponible en Internet: http://observador.pt/2015/08/27/tribunal-constitucional-chumba-acesso-das-secretas-a-dados-bancarios-e-de-comunicacoes/ [documentos consultados: 03 de julio de 2017].

[1726] Es la misma filosofía que está en la base de los datos bancarios a través de la red de control *SWIFT* (*Society for Worldwide Interbank Financial Telecommunication*), en luchar contra el terrorismo, el control y la clasificación de los individuos, sin tener en cuenta el tamaño de los daños a las libertades que pueden derivar

217. Los Estados miembros pueden adoptar medidas legislativas para restringir el acceso de los interesados a sus datos personales, siempre que dichas medidas sean justificadas, necesarias y proporcionadas, y que cumplan con la Carta y el CEDH, tal como se interpreta en la jurisprudencia del TJUE y del TEDH[1727]. En su acción jurisprudencial, el TJUE refuerza la importancia de un alto nivel de protección de los derechos fundamentales cuando los datos se tratan en relación con la seguridad nacional y asuntos policiales[1728]. Antes de la Directiva sobre protección de datos en materia policial, este campo no estaba regulado de manera uniforme en la UE. En este sentido, la Directiva integra parcialmente los criterios establecidos por los TJUE y TEDH, que se pronunciaron en contra de la vigilancia masiva de los datos por parte de las autoridades públicas, en particular nos referimos a los considerandos 18[1729] y 33[1730], y artículo 7 de la Directiva. Este último artículo, como ya se ha indicado, establece que "los Estados miembros dispondrán que los datos personales basados en hechos se distingan, en la medida de lo posible, de los datos personales basados en apreciaciones personales". Por lo tanto, deben adoptarse medidas que garanticen que los datos personales que «*sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros, para lo cual se controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de tercero*»[1731].

para las personas de todo el mundo. Así como no recordar las más famosas "herramientas útiles" contra el terrorismo, que pasaron a primer plano en los últimos años, como el caso de *Wikileaks* de 2010, el caso de *Datagate* de 2013, y con la revelación de las interceptaciones del *NSA* contra los líderes políticos europeos, con lesión grave y evidente del derecho a la privacidad.

[1727] Considerando 46 de la DIRECTIVA (UE) 2016/680.

[1728] TJUE (Gran Sala), *Digital Rights Ireland Ltd y otros*, apartado 37, y TJUE (Gran Sala), *Maximillian Schrems contra Data Protection Commissioner*, apartado 94.

[1729] Considerando 18 de la DIRECTIVA (UE) 2016/680: «*Para evitar que se produzcan graves riesgos de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de los datos personales, así como a su tratamiento manual si los datos personales están contenidos o destinados a ser incluidos en un fichero. Los ficheros o conjuntos de ficheros y sus portadas que no estén estructurados con arreglo a criterios específicos no deben incluirse en el ámbito de aplicación de la presente Directiva*».

[1730] Considerando 33 de la DIRECTIVA (UE) 2016/680: «*Las referencias de la presente Directiva al Derecho de un Estado miembro, a una base jurídica o a una medida legislativa no requieren necesariamente la existencia de un acto legislativo adoptado por un Parlamento, sin perjuicio de los requisitos exigidos por el ordenamiento constitucional del Estado miembro de que se trate. No obstante, dicho Derecho de un Estado miembro, base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para quienes estén sujetos a la misma, tal y como exige la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos. Cuando en el Derecho de un Estado miembro se regule el tratamiento de los datos personales dentro del ámbito de aplicación de la presente Directiva, se deben indicar al menos los objetivos del tratamiento, los datos personales que serán objeto del mismo, la finalidad del tratamiento, los procedimientos para el mantenimiento de la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción, proporcionando con ello garantías suficientes frente a los riesgos de abuso y arbitrariedad*».

[1731] Artículo 7, apartado 2, de la DIRECTIVA (UE) 2016/680.

218. El tratamiento de los datos ha de ser lícito en la medida en que sea «*necesario para el desempeño de una función de interés público llevada a cabo por una autoridad competente en virtud del Derecho de la Unión o de un Estado miembro*» con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, «*incluidas la protección y la prevención frente a las amenazas para la seguridad pública*»[1732]. Tales actividades deben incluir la protección de los intereses vitales de la parte interesada. Para ello deberán indicarse, «*al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento*»[1733]. Los Estados miembros dispondrán que, en los casos en que el Derecho de la Unión o del Estado miembro aplicable a la autoridad competente para la transmisión establezca condiciones específicas para el tratamiento, «*la autoridad competente transmisora deberá informar al destinatario al que se transmitan los datos de las condiciones y la obligación de respetarlos*»[1734].

219. El análisis de los aspectos más relevantes examinados de la Directiva (UE) 2016/680, nos hacen entender que un umbral más bajo de la protección de los datos personales y de los derechos fundamentales en general, de hecho, puede conducir a una recopilación indiscriminada y un uso poco ortodoxo de bases de datos, a una puesta en peligro del derecho a la libertad individual. La única forma de evitar tal eventualidad es la adopción de altas garantías comunes y un menor margen de discrecionalidad para los Estados miembro, precisamente uno de los aspectos criticados en la medida en cuestión. En conclusión, a pesar de que la Directiva promete un progreso en cuanto a las normas europeas de protección de datos en el ámbito penal, no ha conseguido poner punto final a la fragmentación de normas que existe actualmente. Cabe destacar que el equilibrio adecuado entre la seguridad y protección de datos sólo puede alcanzarse mediante el establecimiento de un marco común de referencia, en un reglamento, para el sistema de protección de datos en el ámbito penal. El riesgo de incumplimiento de las normas de protección de datos es mayor cuando hay 28 sistemas nacionales de aplicación diferentes. El respeto de los principios de protección de datos afirmados por el TJUE se hace más difícil de actuar en esa situación. Por lo tanto, estamos a la espera de ver cómo se va a transponer la Directiva en la práctica y qué espacio de maniobra se dejará a las autoridades de protección de datos y a la sociedad civil para que puedan desempeñar sus papeles como guardianes de los derechos.

[1732] Considerando 35 de la DIRECTIVA (UE) 2016/680.
[1733] Artículo 8, apartado 2, de la DIRECTIVA (UE) 2016/680.
[1734] Artículo 9, apartado 3, de la DIRECTIVA (UE) 2016/680.

220. Por lo tanto, no es el momento ahora de ser escéptico con respecto al contenido de la Directiva y si va a tener un impacto real en la legislación. Será el futuro el que mostrará cómo los Estados han implementado las normas de la Directiva en sus respectivas legislaciones y cómo las interpretaciones difieren entre sí.

CONCLUSIONES

1. Los ataques terroristas de los últimos años reavivan de forma periódica un debate que siempre gira en torno a la misma pregunta, como si fuera un requisito ineludible y el punto de partida necesario de cualquier razonamiento sobre el tema: ¿Es necesario renunciar a más privacidad para garantizar una mayor seguridad? La adopción de medidas de seguridad por parte de los sistemas democráticos es una reacción que podríamos definir como funcional para hacer frente a las amenazas que se ciernen sobre la seguridad de sus ciudadanos. Así, los ataques en contra de la seguridad nacional suelen dar lugar a la aprobación de normativa y la adopción de medidas ejecutivas que, por lo general, suelen ser muy restrictivas de los derechos individuales para garantizar una lucha eficaz contra el terrorismo. La situación de emergencia sirve así como factor legitimador de la promulgación de leyes y otras disposiciones de carácter extraordinario que, sin embargo, carecen del requisito de temporalidad, que es connatural a su carácter extraordinario. En efecto, para que una situación de emergencia puedar ser definida como tal, de hecho, es necesario identificar parámetros temporales precisos, más allá de los cuales la acción extraordinaria del Estado ya no puede considerarse legítima. Entre esas medidas carentes de cobertura, los gobiernos han impulsado la obtención generalizada de información y la creación de grandes bases de datos de datos manejados tanto por operadores públicos como privados, con fines de seguridad y prevención de los delitos. Así ha ocurrido de forma sistemática en los EE.UU. después de los ataques terroristas del 11-S de 2001, lo que terminó extendiéndose al continente europeo como consecuencia de los atentados de Madrid en 2004 y Londres en 2005. Posteriormente, los atentados terroristas de Bruselas y Niza de 2016 han impulsado de nuevo a la UE a adoptar medidas legislativas para mejorar la eficacia en el "intercambio de información entre las distintas autoridades nacionales e internacionales y conseguir, a su vez, una mejora en la operatividad de las bases de datos y los sistemas de información".

Se trata, sin duda, de un tema de enorme trascendencia ya que las acciones terroristas en un mundo globalizado plantean un desafío complejo, que no se limita a la acción policial, sino que tensiona las bases mismas del constitucionalismo moderno. De hecho, se trata de un fenómeno –en sus diversos significados– caracterizado por una dimensión histórico-política que, por una parte, busca acabar con el propio Estado de Derecho y, en segundo lugar, provoca la imposición de limitaciones en el disfrute de los derechos individuales tradicionales. En estos términos puede entenderse que, en las últimas décadas, haya una profunda transformación en el modo de combatir el terrorismo internacional por parte de las

autoridades públicas, nacionales e internacionales, con la creación de un sistema de vigilancia masivo, que se justifica por la necesidad de almacenar datos personales no sólo para fines comerciales, sino también con el fin de luchar contra el fenómeno del terrorismo internacional. Estos datos obtenidos y tratados pueden ser usados para construir perfiles detallados de los ciudadanos que se someten a un control por razones de seguridad con métodos cada vez más invasivos. En este contexto, las distintas modalidades de la restricción de la privacidad en nombre de la lucha contra el terrorismo plantean un problema de primer orden que lleva a cuestionar si será posible mantener la privacidad de los datos en un mundo globalizado y en constante evolución, caracterizado por una temible combinación de factores como son la creciente utilización de medios tecnológicos que permiten recabar y manejar cada vez más datos, y la urgencia de adoptar medidas que mejoren la lucha contra la amenaza terrorista.

La obtención de datos a gran escala presenta riesgos ya que puede derivar en una injerencia excesiva en la esfera personal, al margen de que el propio Estado o sujetos no autorizados puedan usar esos datos de forma espuria. El problema no es la incapacidad del individuo para ocultar los hechos a los demás, sino su incapacidad para controlar cómo se utilizan sus datos. El uso de esos datos derivados de la vigilancia genera un problema de desequilibrio de poder, y, en etos términos, la privacidad no puede quedar anulada por el Estado ni tampoco puede ser entregada incondicionalmente a éste.

Así están las cosas, tanto los Estados como la sociedad civil, todos estamos llamados a cuestionar la consistencia en términos legales de las medidas para garantizar la seguridad individual y colectiva y la integridad del Estado mismo. Desafortunadamente las acciones terroristas sacuden de forma periódica a la opinión pública y dan lugar a nuevos capítulos en el debate entre la seguridad y los derechos a la privacidad que cada vez surge con mayor dramatismo, cuando lo que se requiere es una reflexión lúcida y un planteamiento a largo plazo. Las libertades negativas tradicionales –desde la libertad personal– son las primeras víctimas del endurecimiento de las medidas de seguridad ya que resultan progresivamente reducidas hasta cuestionar la existencia misma del Estado de Derecho.

Ante esta dinámica debe recordarse que, cuando un derecho fundamental debe verse afectado por razón del interés general, se requiere un especial equilibrio y proporcionalidad para garantizar un tratamiento normativo adecuado. Este equilibrio resulta complejo ya que las normas en las que se reconocen esos derechos fundamentales son vagas e imprecisas y es

necesario adecuarlas al caso concreto. En este sentido, el equilibrio entre los derechos fundamentales de las personas y la necesidad de las autoridades de obtener datos para fines de seguridad exige responder a preguntas que no tienen una respuesta fácil como, por ejemplo, hasta dónde se deben limitar las medidas que pueden favorecer la seguridad colectiva cuando afectan a los derechos de las personas. En especial cuando, tras un atentado terrorista se plantea la duda de si se hizo lo suficiente para evitarlo, incluso, si las normas de protección de datos europeas y nacionales constituyen un obstáculo para unos Estados que cada vez perciben un mayor riesgo. Frente a esto se revela esencial la obtención eficaz de datos y el intercambio de información y la cooperación flexible entre las autoridades de diferentes países.

La necesidad de un mayor control y prevención por razones de seguridad afecta cada vez más a la protección de las libertades fundamentales en todas sus dimensiones y, en especial, en la que tiene que ver con los datos personales en la era digital. Esta incidencia se ha intensificado desde comienzos del presente siglo como consecuencia de los sucesivos ataques terroristas y, asimismo, por los avances tecnológicos que permiten la adopción de nuevas medidas que, de forma incremental, inciden gravemente en la privacidad de los ciudadanos. En efecto, el perfeccionamiento de las medidas de policía tradicionales se ha visto recientemente acompañado por la introducción de nuevos instrumentos y el fortalecimiento de las medidas de vigilancia y prevención, que intensifican la necesidad de protección de los datos personales. La ampliación de las medidas de obtención de datos como –por ejemplo, la instalación de sistemas de videovigilancia–, ha venido acompañada de una capacidad para crear grandes bases de datos con fines de seguridad, y de nuevas funcionalidades para procesar todos estos datos agregando y analizando grandes cantidades de datos a través nuevas tecnologías. Por ejemplo, los Estados miembros de la Unión Europea proporcionan a terceros países (EE.UU., Canadá, Australia) los datos del registro de nombres de los pasajeros (*Passenger Name Record, PNR*), cuya recopilación y almacenamiento es una medida muy discutida a nivel europeo, ya que se considera escasamente compatible con los principios de necesidad y proporcionalidad que rigen en el tratamiento de datos personales. En este sentido, el propio Parlamento Europeo rechazó una propuesta inicial para establecer la obtención de datos *PNR* para Europa, aunque tras los atentados terroristas de París en 2015, la Directiva *PNR* fue reactivada por la Unión Europea y aprobada como Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (*PNR*) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y

de la delincuencia grave. Esta Directiva prevé la formación de una enorme base de datos que contiene información detallada de todos los pasajeros de vuelos aéreos cuya salida o destino se encuentra dentro del territorio europeo. Los problemas sobre esta medida surgen de una manera más clara por el hecho de que autoridades de terceros países donde las garantías de la privacidad pueden ser menores, también tienen acceso a este registro.

Como muestra la investigación, las medidas adoptadas por la mayoría de los Estados miembros de la Unión que afectan a derechos y libertades fundamentales por razones extraordinarias de seguridad en situaciones de emergencia, se han perpetuado y se mantienen en condiciones de normalidad, y así los ordenamientos internos ofrecen amplias posibilidades a las autoridades de limitar el alcance de los derechos o su ejercicio en interés de la seguridad. Desde el marco de la UE, existe un conjunto de límites a esa capacidad de los Estados de adoptar decisiones en materia de seguridad pública, y en particular, esos límites proceden del respeto a los derechos fundamentales como el derecho a la privacidad, que es común al constitucionalismo europeo y fundamento de la UE. En efecto, el reconocimiento generalizado del derecho a la vida privada en diferentes textos legales analizados en esta investigación son prueba fehaciente de que la protección de la privacidad es un principio ya bien arraigado en el derecho europeo e internacional, sin perjuicio del debate que se aborda a lo largo de la investigación, entre privacidad y control, esto es, el problema de equilibrar los principios de libertad y seguridad en un Estado de Derecho.

2. La privacidad de los individuos y, más concretamente, la protección de sus datos personales se ha constituido, ahora más que nunca, en un elemento central en la agenda político-institucional a nivel mundial. En este debate Europa tiene una oportunidad extraordinaria para liderar y ser un referente en este ámbito, más aún ahora que ha logrado completar, por fin, el largo y complejo proceso legislativo que le ha llevado a dotarse de un nuevo marco jurídico para la protección de los datos de carácter personal que alcanza, aunque no directamente, el ámbito de la investigación penal. A estos efectos, se ha desarrollado un "paquete de reformas" bien estructurado, propuesto en 2012 por la Comisión Europea, que consiste en un Reglamento General de Protección de Datos (UE) 2016/679 para regular el tratamiento de datos personales en los Estados miembros y una Directiva (UE) 2016/680 sobre el uso de datos con fines policiales y judiciales. Esta iniciativa pone de manifiesto la vocación de positivizar el derecho a la privacidad y la necesidad de garantizar una protección homogénea en todo el territorio europeo. La reforma, presentada después de

un largo recorrido de trabajos preparatorios, recibió un intenso apoyo político de varios Jefes de Estado y de Gobierno de la UE, que facilitaron su aprobación finalmente en 2016.
Los fundamentos que han llevado a la Comisión Europea a tomar medidas en este ámbito a través de un "paquete" tan ambicioso, que ha dominado la agenda política europea durante años, se pueden resumir en, al menos, cuatro elementos.

A) La urgente necesidad de proceder de forma inmediata a una segunda, y más intensa, armonización del contenido de la Directiva de 1995 sobre el tratamiento de datos personales y de la Decisión Marco 2008/977/JAI. La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, ciertamente logró el objetivo de una primera armonización en esta materia. La Directiva 95/46/CE ha sido el principal instrumento de la legislación en materia de protección de los datos personales en la Unión, en tanto establecía unas condiciones generales para la licitud del tratamiento de datos personales y definía los derechos de los interesados, todo ello garantizado por unas autoridades nacionales de control independientes. La Directiva definió una serie de cuestiones que quedaban excluidas de su ámbito de aplicación material. Por lo tanto, sus normas no se aplicaban al tratamiento de datos personales efectuados en el ejercicio de actividades que estaban fuera del marco de aplicación del Derecho comunitario y al tratamiento de datos destinados a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.
Por su parte la Directiva, regulaba las excepciones y limitaciones de los derechos y obligaciones de protección de datos, consintiendo que tales limitaciones salvaguarden "la seguridad del Estado", "la defensa", "la seguridad pública", "la prevención", "la investigación", "la detección y la represión de infracciones penales", *etc*. Sin embargo, en el momento de su implementación y posterior desarrollo, los Estados miembros transpusieron su contenido con importantes divergencias, aprovechando al máximo (y en algunos aspectos, de manera muy discutible) el nuevo margen de maniobra ofrecido, interpretando y desarrollando los parámetros europeos en términos bastante distintos. El resultado fue una marcada diversidad de normas y niveles de protección de las personas, una diversidad que sólo era parcialmente justificable sobre la base de las supuestas particularidades culturales, políticas y normativas de los Estados miembros. Esto ha dado lugar a una percepción de asimetrías de protección entre los ciudadanos europeos, así como a incoherencias y dificultades para las empresas que operan a escala mundial. Según la Directiva 95/46/CE, las leyes europeas de protección de datos no son de aplicación en aquellos casos en los que el tratamiento de datos tenga un fin de seguridad pública, defensa, seguridad del Estado y

actividades del Estado en el ámbito penal. Esta disposición se ha convertido, desde el principio, en un obstáculo cada vez que la UE ha intentado incorporar un nuevo instrumento de intercambio de datos en el campo de la seguridad pública.

En 2008, el paradigma cambió con la adopción de la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que regula la protección de datos con arreglo al antiguo tercer pilar. Se trata de un ámbito que no se contempla en la Directiva 95/46/CE, y que se aplica al tratamiento de datos personales en el marco del antiguo primer pilar. "La Decisión Marco sólo se aplica a los datos policiales y judiciales intercambiados entre Estados miembros, autoridades y sistemas conexos de la Unión, sin que se incluyan los datos nacionales". Aunque tal instrumento mejoró la situación de aquel momento, lo cierto es que la Decisión Marco 2008/977/JAI fue objeto de numerosas críticas por ser demasiado ambigua y dejar un margen de discreción muy amplio para la implementación de los Estados miembros.

B) El desarrollo incesante y frenético de las nuevas tecnologías que cambian radicalmente nuestras sociedades. El legislador no debe perseguir la evolución tecnológica con reglas cada vez más detalladas que, al mismo tiempo, se vuelvan rápidamente obsoletas. Sin embargo, la evolución de Internet y las grandes redes, el enorme y creciente flujo de información personal en todo el planeta, la externalización con socios ubicados en cualquier parte del mundo, la computación en la nube, las redes sociales, los motores de búsqueda y, por último, los fenómenos de "*Big Data*" y las nuevas técnicas de vigilancia masiva, han puesto en evidencia todos los límites de la regulación europea anterior. De hecho, la velocidad con la que este sector evoluciona, vinculado a una variedad de intereses económicos, sociales, legales y culturales, hace que el objeto de la regulación sea extremadamente difícil, también debido a la imprevisibilidad de los desarrollos a corto o medio plazo. Al mismo tiempo, dado que el progreso tecnológico no puede ni debe detenerse, se hace necesario canalizar esta fuerza innovadora hacia un uso consciente y provechoso, que sea beneficioso y no perjudicial para la evolución de las sociedades modernas. Es precisamente a la luz de esta complejidad y la necesidad de ofrecer herramientas reglamentarias adecuadas como tiene que leerse el nuevo marco normativo sobre la protección de datos personales.

C) El nuevo marco jurídico derivado del Tratado de Lisboa. La introducción de una regulación europea para proteger eficazmente a todas las personas (no sólo a los ciudadanos

europeos) en relación con el tratamiento de los datos que les conciernen por parte de las instituciones europeas, de los Estados miembros y cualquier entidad pública o privada que trate datos personales, se convierte en una obligación jurídica de la Unión, así como garantiza su protección (independientemente de la jurisdicción) por parte de las autoridades independientes.

El Tratado y la CDFUE han elevado el derecho a la protección de los datos al rango de derecho fundamental autónomo, separado del derecho tradicional a la protección de la vida privada. Cada individuo tiene reconocido dicho derecho fundamental independientemente de la existencia de normas más específicas que lo desarrollen, ya que el mismo es exigible, como tal, a nivel jurisdiccional en toda la Unión. Otro tanto ocurre, en segundo lugar con el CEDH, independientemente de la compleja incorporación de la Unión: «*La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos* (…)». Además, el TUE establece que «*Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales*» (artículos 2 y 6 del TUE). Esto implica la necesidad de que la UE tome medidas ahora para cumplir con las obligaciones positivas derivadas del CEDH que, de conformidad con el artículo 8, exige utilizar los instrumentos normativos adecuados para evitar que entidades tanto públicas como privadas interfieran de manera no necesaria o no proporcionada en la esfera privada de las personas y su derecho a una protección adecuada de los datos que les conciernen.

D) La importancia del trabajo hermenéutico jurisprudencial llevado a cabo por los Tribunales supranacionales (TJUE y TEDH). En el ámbito europeo, el derecho a la privacidad ha evolucionado y se ha reafirmado de manera muy decisiva, en un diálogo constante entre el legislador y los tribunales que ha permitido ampliar el alcance del derecho a la privacidad, incluso en un contexto adverso derivado de las amenazas a la seguridad. En los últimos años, es posible identificar una serie de sentencias del TJUE, unidas no sólo por el mismo ámbito de intervención, a saber, el derecho a la protección de datos personales, sino también, y, sobre todo, por compartir una misma aplicación de determinadas técnicas de toma de decisiones y una interpretación de la CDFUE capaz de exigir algunas reflexiones de carácter general con respecto al papel desempeñado por la propia Carta y, al mismo tiempo, en relación con el TJUE. El Tribunal ha dictado en los últimos años algunas sentencias con un impacto significativo sobre la cuestión del difícil equilibrio entre derechos

y las políticas de seguridad implementadas hasta el momento por los Estados. Estas sentencias, algunas de las cuales se han analizado durante la investigación, muestran cómo gracias al TJUE, sobre la base de la CDFUE, la protección de los datos personales tiene ahora la fisonomía clara e inequívoca de un derecho fundamental, capaz de prevalecer en sectores con una larga tradición de intervenciones estatales, como la seguridad pública y la seguridad nacional. Cuando el Tribunal juzga la validez de los actos de Derecho derivado, utiliza los artículos 7 y 8 de la Carta como parámetros de validez autónomos e independientes, aparte de la remisión a otras fuentes de los Tratados o el Derecho derivado. El Tribunal no se limita a mencionar en términos generales la CDFUE; por el contrario, la autosuficiencia de la Carta emerge claramente como un parámetro de legitimidad y aplicación autónoma de sus disposiciones sobre derechos fundamentales. Por lo tanto, la afirmación de la centralidad de los artículos 7 y 8 de la CDFUE en la jurisprudencia citada es clara e incontestable: en el fallo *Digital Rights Ireland*, estas disposiciones de la Carta son el eje sobre el cual el Tribunal justifica la anulación de una Directiva; en *Schrems*, las disposiciones se aplican como un parámetro incluso hacia una normativa de un país extranjero, como los EE.UU., a la que la Decisión de la Comisión Europea se refería; en *Tele2 Sverige*, las disposiciones para la protección de la privacidad digital se utilizan para reafirmar la prevalencia de la protección de datos sobre las instancias de seguridad del Estado invalidando de hecho la normativa estatal, con el efecto indirecto de reafirmar la centralidad del TJUE en su papel de depositario de la Carta y la aplicación unívoca y homogénea del Derecho de la Unión en todos los Estados miembros.

En su jurisprudencia, el Tribunal ha identificado un núcleo fuerte de derechos fundamentales inviolables a nivel europeo, que incluye la protección de la vida privada y los datos de las personas. Una protección que presenta características expansivas si consideramos que, en la jurisprudencia antes mencionada, todas las cláusulas que salvaguardan la autonomía del Estado fueron interpretadas por el Tribunal de Luxemburgo de manera restrictiva. Es significativo que esta interpretación se plantee, una vez más, en un caso relacionado con el equilibrio entre las instancias de seguridad, prevención y persecución de delitos, por un lado, y la protección del derecho fundamental a la privacidad, por el otro. Esto es lo que sucedió no sólo en *Digital Rights Ireland* sino también en *Schrems*, donde, junto con los perfiles económicos vinculados a grandes empresas de la web, el núcleo del problema eran las necesidades de investigación y de inteligencia de las autoridades federales estadounidenses. En ambas sentencias, el Tribunal emite un juicio de validez de un acto de derecho derivado, actuando en la práctica como un juez constitucional. Del mismo modo, incluso en el caso *Tele2 Sverige*, aunque no formalmente, el TJUE ha aplicado un razonamiento y ha

desarrollado un tipo de pronunciación que toma la sustancia (pero no la forma) de una verdadera declaración de invalidez, con clara analogía con *Digital Rights Ireland* y de manera similar a lo que ya sucedió en *Schrems*.

No debemos olvidar el contexto histórico, social y político en el que se han dictado estas sentencias que, ciertamente, muestra una preocupación generalizada por el abuso de ciertas técnicas de vigilancia masiva, como aquellas dirigidas a la conservación masiva e indiscriminada de datos personales. En las tres sentencias analizadas, se hace referencia a los "principios de necesidad y proporcionalidad" del tratamiento. En *Digital Rights Ireland*, *Schrems* y *Tele2 Sverige*, con referencias cruzadas a la primera decisión de los dos últimos, se afirma que la protección del derecho fundamental a la privacidad requiere en todo caso que las excepciones y restricciones a la protección de datos personales establecidas por los Estados deben estar dentro de los límites de lo "estrictamente necesario". La referencia al principio de proporcionalidad y necesidad aplicado por el Tribunal al legislador europeo y estatal coincide, por tanto, en el lenguaje de protección de datos, con el principio de necesidad y proporcionalidad del tratamiento de datos, en el sentido de que el Tribunal, afirmando que las normativas estatales sobre conservación de datos deben limitarse a lo "estrictamente necesario", refleja el principio de necesidad del tratamiento de datos regulado en la anterior Directiva de 1995 (artículo 7) y ahora en el nuevo RGPD (artículo 5, apartado 1) como la "minimización de los datos" y la "limitación del plazo de conservación", que se convierte en una prueba de proporcionalidad de la intervención pública. Esto permite al Tribunal, en materia de derechos fundamentales, entrar a evaluar el margen de discrecionalidad de las intervenciones estatales, gracias a la prueba de proporcionalidad. Con su actividad, el TJUE consagra el derecho a la privacidad, reconociéndolo como la promulgación directa de dos disposiciones de la CDFUE y elevando el rango de la disciplina contenida en las directivas sobre privacidad y, ahora, el nuevo Reglamento. Asimismo, y de forma simultánea, los principios fundamentales de la protección de datos se explican sobre todo en el principio de proporcionalidad, tal como se establece en el primer apartado del artículo 52 de la Carta de Niza.

Si el TJUE ha aumentado en los últimos años su atención a los derechos fundamentales –especialmente desde el Tratado de Lisboa en adelante, como resultado de la "constitucionalización" definitiva de la CDFUE–, es sin duda por la influencia ejercida por el Tribunal Europeo de Derechos Humanos, fuente de décadas de experiencia en el campo de la defensa de los derechos inviolables de la persona. También en la jurisprudencia del Tribunal de Estrasburgo existen límites sólidos para la proliferación de restricciones al

disfrute de las libertades debido al fortalecimiento de las políticas de seguridad. El TEDH desde siempre ha prestado especial atención a la protección del "Derecho al respeto a la vida privada y familiar" (como se establece en el artículo 8 del CEDH de 1950), especialmente en relación con la prevención y detección o enjuiciamiento de infracciones penales, así como de seguridad.

En este sentido, en *Roman Zakharov contra Rusia*, sentencia de 4 de diciembre de 2015 el Tribunal sostuvo que las normas internas que rigen la interceptación de comunicaciones no ofrecían garantías adecuadas y efectivas contra la arbitrariedad y el riesgo de abuso. El Tribunal declaró que el Estado ruso había violado el artículo 8 del CEDH en relación con el marco legal que regulaba las medidas de vigilancia secreta de las comunicaciones, y, en concreto, las garantías necesarias que debían regir dichas medidas. Con particular referencia a la delicada relación entre la seguridad y la privacidad, es de especial importancia la sentencia dictada el 12 de enero de 2016 en el procedimiento *Szabo y Vissy contra Hungría*. En particular, el Tribunal, aunque reconoció que la normativa húngara sobre vigilancia antiterrorista secreta introducida en 2011 era una consecuencia natural de las formas adoptadas por el terrorismo actual que los gobiernos recurrieran a tecnologías de vanguardia, incluida la supervisión masiva de las comunicaciones, para prevenir incidentes inminentes, ha sido especialmente severo censurando el sistema de orden de registro intrusivo, interceptación y grabación que la legislación húngara introdujo sin proporcionar garantías adecuadas para la protección de la persona. En concreto, la ley antiterrorista permitía en la práctica una actividad de vigilancia indiscriminada. Además, la adopción de tales medidas se realizaba sin una evaluación independiente sobre si tales medidas eran estrictamente necesarias. Todo eso acompañado por un periodo esencialmente ilimitado de medidas de control, en ausencia de cualquier forma de supervisión judicial a tutela de eventuales abusos. En este caso, el Tribunal sostuvo que hubo una violación del artículo 8 del Convenio enfatizando el valor persistente de los principios de necesidad, finalidad y proporcionalidad en un momento histórico muy crítico, cuando los derechos inviolables de la persona se encontraban bajo los ataques terroristas, pero también, como consecuencia, se exponían al riesgo de suspensión o minimización por parte de las mismas autoridades públicas que se encargan de la defensa frente a estos ataques.

De este modo la acción pretoriana combinada, tanto del TJUE como del TEDH con decisiones de impacto interno e internacional extraordinariamente importantes, han frenado los intentos de fortalecer los instrumentos de seguridad que habrían podido derivar en un repliegue excesivo del derecho a la privacidad. En cuanto respecta a la cuestión de la

privacidad, por tanto, estos Tribunales supranacionales han intervenido recientemente casi al unísono en defensa de este derecho fundamental potencialmente en riesgo. También, al mismo tiempo, facilitaron claras indicaciones a los legisladores, estableciendo los principios de una manera decididamente detallada, de modo tal que permitieran su incorporación en actos legislativos posteriores adoptados a nivel europeo, como es el caso, precisamente, del nuevo paquete de reformas europeas aprobado en 2016.

Este "activismo" por parte de estos dos tribunales se debe, sin embargo, a la falta de iniciativa política. Las decisiones jurisprudenciales se sobreponen y prevalecen sobre las políticas legislativas. Y la evaluación de la conciliación de valores y derechos en juego se excluye de las instancias de la representación y este equilibrio se confía al arbitrio judicial. De hecho, la jurisprudencia traza el camino y la política, en la práctica, lo sigue. Por ejemplo, sólo después de la anulación de la Directiva europea sobre retención de datos de 2006, los legisladores nacionales han intervenido sobre la normativa sobre la protección de la privacidad, a veces por un impulso adicional de los jueces nacionales o constitucionales, que también han tenido que entrar a resolver sobre los términos de este debate. Por lo tanto, aspectos críticos de la configuración del ordenamiento jurídico se dejan permanentemente a la voluntad de los jueces. La privacidad está mal garantizada por los responsables políticos, nacionales e internacionales, que operan, en el mejor de los casos, como reacción ante acontecimientos terroristas o como consecuencia de decisiones judiciales, nacionales y supranacionales, sin las cuales por lo general permanecerían impasibles. A este respecto conviene recordar, entre muchos casos, la aprobación, en abril de 2016, después de los ataques de Paris y Niza, de la Directiva europea *PNR*, relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave; o la aprobación, en julio de 2016, del acuerdo de adecuación para las transferencias de datos a EE.UU. denominado "*Privacy Shield*" ("Escudo de la privacidad"), tras la sentencia del TJUE sobre el caso *Schrems*. Este activismo garantista de los jueces se despliega cuando se trataba de la violación de la privacidad por manos de otras autoridades públicas, que lleva a la sustitución de los decisores públicos o a la apertura de brechas en el sistema que requieren una acción urgente para llenar el vacío normativo creado.

En esta dinámica, el legislador es incapaz de adoptar decisiones fuertes, inequívocas y suficientemente estables. Clara muestra de este fenómeno son, por ejemplo, los siguientes casos: 1) después la declaración de nulidad de la Directiva sobre conservación de datos por el Tribunal de Justicia en 2014, aún no se ha sustituido la Directiva anulada; 2) la larga espera para la aprobación del "paquete de reformas" que, según la doctrina más autorizada,

es una reforma "nacida vieja" y con fuertes límites que han sido sólo parcialmente resaltados. Finalmente, debe tenerse en cuenta que ningún derecho fundamental, incluido el derecho a la privacidad, puede dejarse a la sola interpretación judicial para que decida ella misma sobre los límites y restricciones y, en definitiva, sobre la configuración del derecho en cuestión. Y tampoco parece razonable que sean los tribunales los que, desde esta posición de supremacía, determinen el equilibrio entre libertad y seguridad.

3. Con referencia a la reforma del marco de protección de datos, en la transición de la vieja normativa a la nueva, debe destacarse el papel desempeñado, en particular, por la Comisión y el Parlamento (colegislador, junto al Consejo) y, a partir de mayo de 2018, por todos los Estados miembros de la UE que dispondrán de una única normativa homogénea en una cuestión que afecta a un derecho fundamental. La reforma de la protección de datos en Europa (Reglamento y Directiva, concebidos como "paquete" indivisible) responde a una elección de fortalecimiento de los derechos y garantías que no ha descuidado aportar elementos de innovación.

A) La aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido largamente esperada y recibida con un sentimiento general de optimismo. Para muchos, la introducción de una disciplina general, mediante la adopción de un acto vinculante y autoejecutivo (artículo 288 del TFUE), parecía la respuesta adecuada a la dinámica de nuestro tiempo, marcada por la vertiginosa evolución y revolución del contexto en el que el derecho a la protección de datos personales opera. Si el descenso a los detalles al ordenar una materia puntual conlleva el riesgo de una desactualización acelerada, la provisión de obligaciones específicas y rigurosas para los sujetos que asumen el tratamiento de los datos personales ("responsable y encargado") puede suponer una garantía efectiva de una evolución interpretativa proyectada hacia el futuro, pero firmemente anclada en los principios fundamentales de la materia. En cualquier caso, el RGPD parece brindar respuestas oportunas a problemas específicos, identificando los problemas y las principales lagunas del pasado e intentando proporcionar herramientas que garanticen un alto nivel de protección.

En este sentido, resulta interesante el claro cambio de perspectiva de toda la disciplina marcada, ahora, en la máxima prevención de daños y perjuicios a los derechos fundamentales que podrían resultar de una violación de las medidas de seguridad o un tratamiento ilegal. Esto, sobre todo, se basa en la "definición del tratamiento de datos personales" como una actividad que potencialmente genera riesgos. Sobre todo, existe una obligación general por

el responsable del tratamiento, «*teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas*», de aplicar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento" (artículo 24).

Este enfoque del nuevo sistema de protección se encuentra explícitamente en la introducción de particularidades como la evaluación preventiva, que se implementará cuando exista el riesgo de que el tratamiento conlleve "probabilidad y gravedad para los derechos y libertades de las personas físicas"; o mediante la introducción de los denominados principios de protección "desde el diseño" y por "defecto" ("*privacy by design*" y "*by default*"), gracias a los cuales es posible aplicar todas las medidas necesarias para la protección de datos incluso antes de que el tratamiento tenga lugar, y al mismo tiempo, garantizar que, de forma predeterminada, sólo se traten "los datos personales necesarios para cada fin específico del tratamiento". A diferencia de la legislación anterior, se colocan las medidas de tratamiento y seguridad en el centro de la nueva protección de los datos personales del acto legislativo europeo, cuyo cumplimiento de los principios del RGPD se entiende como un requisito previo esencial para la protección y el ejercicio de los derechos humanos.

La nueva normativa europea también reafirma y refuerza, como la normativa precedente, el papel central del consentimiento, articulado por los deberes de información y transparencia. El nuevo régimen de flujos de datos a terceros países otorga una mayor flexibilidad a los operadores, en comparación con las disposiciones de la Directiva 95/46/CE. Aunque se confirman las decisiones de adecuación como el principal mecanismo para transferir datos fuera de las "fronteras" de la UE, el RGPD incluye también instrumentos alternativos. La efectividad de las nuevas normas sólo se puede evaluar a la luz de la experiencia concreta de aplicación, aunque fijar algunos requisitos mínimos por parte del legislador ayudará a limitar los márgenes de discreción de los operadores y garantizar una mayor transparencia en las operaciones de transferencia de datos personales. En consideración a esto, se puede afirmar que el RGPD ciertamente representa un gran paso adelante en el panorama normativo de la protección de datos personales, no sólo por las innovaciones introducidas, que son ciertamente significativas, sino sobre todo por el fortalecimiento y confirmación de los principios y determinaciones contenidos en las normativas anteriores. En este sentido debe tenerse en cuenta que los retrasos en la aprobación de esta normativa por parte del legislador europeo parecen derivar de la necesidad de considerar la introducción de una gran cantidad de garantías individuales, que podrían ser un obstáculo para la aplicación de las

medidas destinadas a proteger la seguridad colectiva, especialmente bajo limitaciones a la capacidad de circulación de los datos personales. Al contrario de lo que ocurría en la normativa precedente, el RGPD introduce mayores garantías individuales y más obligaciones para los responsables del tratamiento, poniéndose de acuerdo con la óptica garantista del sistema europeo, en una posición dominante la protección de los derechos de los ciudadanos, aunque sea en detrimento de la seguridad colectiva.

La reforma era necesaria ya que la UE responde así al desafío planteado por el creciente intercambio de datos personales y la necesidad de garantizar los derechos a la protección de datos y la privacidad en todos los ámbitos de actuación de la UE. La Unión tiene la tarea de garantizar que el derecho a la protección de datos se aplique de forma "coherente y homogénea". Pero hay que preguntarse si será realmente así. Desde el punto de vista de las fuentes, no cabe duda de que esto ha sido posible gracias al mencionado artículo 16 del TFUE, que hoy es la base jurídica del nuevo Reglamento y Directiva.

El Reglamento trata de superar los límites y defectos de los instrumentos legislativos previos mediante la introducción de mecanismos más eficaces a la hora de garantizar un equilibrio entre la protección de los datos personales y la lucha contra la delincuencia y el terrorismo. En este sentido, el RGPD ha dado como resultado la inaplicación automática de las normas nacionales que se opongan a su contenido, y la consiguiente revisión de todo el conjunto de normas, incluso secundarias, que a nivel nacional desarrollan, especifican, interpretan o introducen excepciones y derogaciones a la normativa europea contenida en la Directiva 95/46/CE –tal y como es, en el caso de España, la LOPD de 1999 o en el caso italiano el "*Codice della privacy*" de 2003–. De todas formas, el Reglamento no se constituirá en "única Ley europea" al respecto ya que contempla categorías de disposiciones a nivel nacional que, de conformidad con el mismo, continuarán contribuyendo activamente a la ordenación de este sector.

En este sentido, con la finalidad de garantizar "un nivel de protección constante y elevado para las personas físicas y eliminar los obstáculos a la circulación de datos personales en la UE, el nivel de protección de los derechos y libertades de las personas físicas con respecto al tratamiento de dichos datos debería ser equivalente en todos los Estados miembros". Conviene garantizar una "aplicación" «*coherente y homogénea*» de las normas que protegen los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales en toda la Unión. Pero esto no ha sido totalmente logrado por el RGPD por varias razones:

1) Con respecto al «*tratamiento de datos personales para el cumplimiento de una obligación legal*», para la ejecución de una tarea llevada a cabo en interés público o en relación con el ejercicio de poderes públicos conferidos al responsable del tratamiento, "los Estados miembros deben permanecer libres y mantener o adoptar normas nacionales para especificar mejor la aplicación de las normas del Reglamento".

2) En lo que respecta «*al tratamiento de datos personales por parte de las autoridades competentes*» a los efectos del ámbito de aplicación del RGPD, los Estados miembros deben poder "mantener o introducir disposiciones más específicas para adaptar la aplicación de las disposiciones del Reglamento". Estas disposiciones pueden determinar con mayor precisión requisitos específicos para el tratamiento de datos personales por parte de esas autoridades competentes para estos otros fines, teniendo en cuenta la estructura constitucional, organizativa y administrativa de los respectivos Estados miembros. Cuando el tratamiento de datos personales se realice por organismos privados dentro del ámbito de aplicación del RGPD, los Estados miembros deberían poder, en determinadas condiciones, adoptar disposiciones legislativas para limitar obligaciones y derechos, siempre que esta limitación constituye una medida "necesaria" y "proporcionada" "en una sociedad democrática" para salvaguardar importantes intereses específicos: la seguridad pública y las actividades de prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y su prevención.

3) El RGPD también reconoce un "margen de maniobra a los Estados miembros para especificar sus normas". En este sentido, el Reglamento «*no excluye el Derecho de los Estados miembros*» a "establecer las condiciones para situaciones de tratamiento específicas", incluso determina de "forma más precisa las condiciones en las que el tratamiento de datos personales es lícito". Los Estados miembros deben poder establecer disposiciones relativas a las sanciones penales por infracciones del Reglamento, incluidas las infracciones de las normas nacionales adoptadas de conformidad con los límites del propio Reglamento. Sin embargo, la imposición de sanciones penales por violaciones de estas normas nacionales y sanciones administrativas no debe entrar en conflicto con el principio "*ne bis in ídem*" tal como lo interpreta el TJUE.

En definitiva, «*la legislación de la Unión o del Estado miembro*» puede "imponer limitaciones a los principios y derechos" específicos de información, acceso, rectificación y supresión de datos, al derecho a la portabilidad de datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfil y la comunicación de una violación de la

seguridad de datos personales y de ciertas obligaciones relacionadas con el tratamiento de datos por el responsables del tratamiento, siempre y cuando sean "necesarias y proporcionadas en una sociedad democrática" para proteger la seguridad pública, incluida la protección de la vida humana, la prevención, investigación y persecución de delitos o la ejecución de sanciones penales, incluida la protección y prevención de los riesgos contra la seguridad pública, para la protección de otros objetivos importantes de interés público general de la Unión o de un Estado miembro. A estos efectos debe recordarse que la seguridad nacional y la seguridad pública son objetivos legítimos, según el CEDH y la CDFUE, para imponer restricciones al derecho a la protección de datos personales bajo ciertas condiciones.

En primer lugar, queda claro que la restricción debe ser necesaria y proporcionada en una sociedad democrática. Evidentemente, recuerda la fórmula contenida tanto en el CEDH como en la CDFUE. En segundo lugar, se prevé que la restricción, adoptada por ley, debe contener algunas disposiciones específicas relativas: a) "las finalidades del tratamiento o las categorías de tratamiento"; b) "las categorías de datos personales"; c) "el alcance de las limitaciones introducidas"; d) "las garantías para evitar abusos o accesos o traslados ilegales"; e) "la indicación precisa del responsable del tratamiento de datos"; f) "los períodos de conservación y las salvaguardas aplicables teniendo en cuenta la naturaleza, el alcance y la finalidad del tratamiento o las categorías de tratamiento"; g) "riesgos para los derechos y libertades de las personas involucradas"; y h) "el derecho de los interesados a ser informados de la limitación, a menos que esto pueda poner en peligro su finalidad". Como se puede entender de las normas antes mencionadas, parece que la prueba de legitimidad sobre las restricciones va a ser muy rígida, en línea con la jurisprudencia más reciente del TJUE y del TEDH que, a pesar de sus diversidades, son referencias inevitables para destacar los límites dentro de los cuales cualquier restricción a la protección de datos personales se considerada legítima.

Finalmente, es cierto que tal vez no se pueda esperar del RGPD medidas más audaces y ambiciosas en el ámbito de la seguridad, sobre todo teniendo en cuenta el contexto en el que este se desarrolla, condicionado por la emergencia terrorista que tradicionalmente es abordada por los Estados de forma individual. Es cierto que este contexto de amenaza y temor constante llevan a demandar medidas estrictas de prevención y policía, favoreciendo la intensificación de los instrumentos de control, incluso si afectan a posiciones legales consolidadas. Sin embargo, incluso en esta situación, un orden democrático nunca puede excederse en la limitación de los derechos fundamentales reconocidos a los ciudadanos, ya

que quedaría comprometida la libertad y la dignidad humana que están en la base del Estado de Derecho. Está claro que nuestro sistema normativo puede tolerar limitaciones a los derechos fundamentales, especialmente si se quiere proteger la seguridad de la población de amenazas graves, pero siempre es necesario identificar la proporcionalidad y la razonabilidad de las medidas utilizadas por las autoridades de seguridad competentes con respecto a los derechos fundamentales, evitando que la limitación no exceda lo que una persona puede legítimamente tolerar.

Con referencia al principio de proporcionalidad, el nuevo RGPD presenta una novedad para su aplicación a la legislación nacional. El artículo 6, apartado 3, última frase del Reglamento establece que «*El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido*». Esta disposición representa la expresión del principio de proporcionalidad transpuesta al legislador estatal, similar de alguna manera a lo que planteó el TJUE en *Tele2 Sverige* y, sin duda, de acuerdo con la cláusula de proporcionalidad del artículo 52 de la Carta de Niza. En otras palabras, sea como proporcionalidad del tratamiento *stricto sensu* o como proporcionalidad de la intervención pública para limitar la privacidad individual, este principio también se confirma como uno de los nuevos elementos presentes en el nuevo Reglamento europeo, aunque con los límites previamente expuestos.

El RGPD también parece acoger el hecho de que la protección de datos es ahora un límite contra los controles ilegales que afectan a nuestra libertad, un interés general fundamental de la Unión Europea. De hecho, después de recordar que el derecho a la protección de datos en tanto que derecho fundamental no es una prerrogativa absoluta, agrega que debe considerarse a la luz de su función social. De hecho, por ejemplo, el Reglamento exige al responsable del tratamiento de datos presentar pruebas a las autoridades de control de que ha tomado todas las "medidas técnicas organizativas apropiadas" para «*garantizar la seguridad del tratamiento*» y para minimizar riesgos, así como el intento del nuevo sistema normativo de fortalecer el grado de protección a través de una serie de innovaciones muy significativas que van desde la responsabilidad proactiva ("*accountability*") de los responsables hasta la obligación de llevar a cabo un análisis de riesgo preventivo con la obligación de adoptar la "protección de datos desde el diseño" y, "por defecto", desde el fortalecimiento dinámico de las medidas de seguridad hasta las normas para informar y gestionar las violaciones de datos. De ello se deduce, por lo tanto, que el legislador europeo con estos actos ha decidido cambiar completamente el punto de vista tradicional de la protección de datos personales, trasladándolo del destinatario de la protección al sujeto que

utiliza activamente esta información. Y es precisamente en esta reorganización que se han redefinido los elementos esenciales de todo el marco regulatorio.

B) Según el RGPD, la protección de las personas físicas con respecto al tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección contra amenazas a la seguridad pública y su prevención, y la libre circulación de estos datos, es objeto de una regulación específica por parte de la Unión, por lo que el RGPD no debe aplicarse al tratamiento llevado a cabo para tales fines. Los datos personales tratados por las autoridades públicas de conformidad con el RGPD, cuando se utilicen para tales fines, se encuentran regulados por una disposición de la Unión más específica, en particular la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. "Los Estados miembros pueden conferir a las autoridades competentes, de conformidad con la Directiva (UE) 2016/680, otras tareas que no se lleven a cabo necesariamente para la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de modo que el tratamiento de datos personales para estos otros fines entra dentro del ámbito de aplicación del RGPD".

Los atentados terroristas de 2001 pusieron de manifiesto la necesidad de intercambiar -en el marco de la cooperación judicial y policial en la lucha contra el terrorismo-, ciertas informaciones relativas a datos personales de determinados individuos. La necesidad de la elaboración de una norma común sobre protección de datos que permita a las autoridades policiales y judiciales "cooperar más eficazmente entre sí, así como fomentar la confianza y garantizar la seguridad jurídica", era urgente y necesaria. La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, intenta remediar esta situación.
La norma tiene el objetivo de garantizar que el nivel de protección de los derechos de las personas sea igual en todos los Estados miembros en relación con el tratamiento de sus datos personales en asuntos policiales. Con la introducción de esta nueva Directiva, se abarcan los principales objetivos y principios del instrumento para el procesamiento de datos; los derechos del interesado y las obligaciones del responsable del tratamiento y las autoridades

nacionales de control; y la protección de datos personales cuando se transmite a terceros países. "La Directiva procede: a) proteger los derechos y libertades fundamentales, especialmente el derecho a la protección de los datos personales; y b) garantizar un elevado nivel de seguridad pública, y al mismo tiempo asegurar el intercambio de datos personales entre las autoridades competentes dentro de la Unión". En todo caso, el contenido de la Directiva es abstracto y necesita aclaración.

Esta Directiva facilita la realización de un área de libertad, seguridad y justicia, al tiempo que uniforma la legislación de protección de datos de los Estados miembros en el campo de los asuntos policiales estableciendo el nivel mínimo de armonización. La Directiva utiliza, en casi todos los artículos, la palabra «*dispondrán*» cuando exige a los Estados miembros implementar reglas en su legislación nacional. Esto es, en parte, el resultado de compromisos entre los intereses respectivos de los Estados miembros. "Su fin es asegurar que el nivel de protección de los derechos de las personas naturales sea igual en todos los Estados miembros en relación con el tratamiento de sus datos personales". Eso significa que los Estados miembros deben proporcionar al menos el mismo nivel de protección en su legislación. La legislación de los Estados miembros sobre protección de datos en asuntos policiales difiere entre sí. Las autoridades nacionales tienen diferentes enfoques sobre los aspectos del tercer pilar. Como ejemplo, algunos países tienen reglas más estrictas sobre el "secreto" y los interesados no tienen posibilidades igualmente amplias de acceder a sus datos personales y algunos sectores de la policía pueden estar fuera de la supervisión. "Las autoridades nacionales pueden interferir con los derechos fundamentales de las personas si se basan en los requisitos de seguridad nacional y de interés público. La lucha contra los delitos graves y el terrorismo es importante para garantizar la seguridad pública y su eficacia puede depender del uso de técnicas modernas de investigación. Pero un objetivo de interés general en sí mismo no justifica una medida de retención de datos indiscriminada y generalizada". Corresponde a las autoridades nacionales y los tribunales interpretar y aplicar principalmente la legislación nacional.

La legislación uniforme de la UE mejora la cooperación entre las autoridades, pero la normativa europea permite a los Estados miembros adoptar legislaciones que difieren entre sí. Esto genera efectos negativos y un trato desigual entre los interesados. Diferentes estándares obstaculizan la cooperación entre las autoridades. Los Estados miembros de la UE todavía dependen de mecanismos de cooperación basados en normas que no tienen en cuenta la evolución de la tecnología. La investigación policial será complicada cuando involucre a varias jurisdicciones ya que la legislación no está armonizada. La Directiva de

protección de datos en materia policíal establece que su finalidad es uniformar el nivel de protección de los derechos de las personas físicas en los Estados miembros en relación con el procesamiento de sus datos personales.

La protección de datos en el ámbito de la policía y de la seguridad tiene que ser coherente con la normativa general contenida en el RGPD y adquirir una naturaleza especial sólo cuando sea estrictamente necesario. De este modo, la nueva Directiva y el RGPD se complementan entre sí, ya que operan en diferentes sectores, pero cooperan en las áreas donde se superponen. Si bien el RGPD establece normas generales para proteger a las personas en relación con el tratamiento de sus datos personales y para garantizar la libre circulación de dichos datos dentro de la UE, la Directiva establece normas específicas para la protección de datos en el ámbito judicial de cooperación en asuntos penales y cooperación policial. Por ejemplo, el RGPD se aplica cuando una autoridad competente revela legalmente datos personales a un destinatario que no es una autoridad competente definida por la Directiva –a este respecto la Directiva armoniza al nivel mínimo–. Cuando una autoridad competente procese datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, se aplicará la Directiva (UE) 2016/680. El hecho de que los Estados miembros puedan adoptar normativa que traspone las disposiciones de la Directiva de manera diferente que otros Estados, puede crear efectos negativos para los interesados y un tratamiento desigual entre los Estados miembros. “La existencia de diferentes estándares de protección de datos complicará el intercambio de información y obstaculizará la cooperación entre las autoridades”, ya que resultará más difícil identificar a las personas involucradas en actuaciones delictivas y obtener pruebas. Por ejemplo, proporcionar a los interesados el mismo nivel de protección en términos de derechos de información, acceso o eliminación de sus datos personales según el RGPD podría significar que cualquier operación de vigilancia llevada a cabo con fines policiales se volvería ineficaz en el contexto de la aplicación de la ley.

La Directiva incluye en su texto la frase «*la protección y la prevención frente a las amenazas contra la seguridad pública*» que puede interpretarse como básicamente cualquier cosa que la autoridad pública nacional considere un peligro, ya sea una amenaza o no. Esta frase constituye la base para introducir excepciones en el tratamiento de los derechos de las personas. Si se considera que “seguridad pública” y “seguridad nacional” son conceptos en evolución, los legisladores no pueden predecir el desarrollo del mundo en el futuro, por lo

que sus significados no deberían estar redactados de manera demasiado estricta en la normativa o podrían limitar la capacidad de interpretación de las autoridades.

Por su parte, los Estados miembros pueden encontrar problemas al trasponer la nueva Directiva en sus legislaciones nacionales: la Directiva permite amplias posibilidades a los Estados miembros para interpretar las disposiciones. En comparación con el procesamiento de datos para fines comerciales, que está contemplado por la regulación, el procesamiento relacionado con la seguridad puede requerir cierto nivel de flexibilidad. Los términos y las condiciones contenidos en la norma europea no son claros y no pueden transcribirse directamente en la normativa nacional, sino que necesitan ser concretados primero. El Estado miembro puede trasponer el contenido de la Directiva de manera diferente que otros, como ya ocurrió en otras normas precedentes, creando efectos controvertidos para los interesados y un tratamiento heterogéneo entre los Estados.

Como consecuencia, "la existencia de diferentes niveles de protección en la normativa de protección de datos complicará el intercambio de información y obstaculizará la cooperación entre las autoridades". La nueva Directiva no armoniza este ámbito tanto como lo haría el RGPD si el Reglamento también incluyera el ámbito de aplicación de la Directiva.

En definitiva, se puede concluir que la Directiva no ha logrado la claridad y el equilibrio necesarios entre la protección de datos y otros intereses legítimos para enfrentar los desafíos terroristas que son particularmente pertinentes en sectores específicos. Como se ha podido comprobar, la seguridad pública y nacional son objeto de un "dominio reservado" de los Estados, a pesar de la perspectiva de realización de un ELSJ que ha acelerado el proceso de armonización de la normativa europea. Cuando los Estados miembros se ven obligados a uniformar sus legislaciones, que se caracterizan por sus propias tradiciones legislativas y culturales, y el instrumento que guía el proceso permite ese margen de maniobra "abstracto", es imposible predecir el resultado "concreto". Una buena intención puede dar lugar a malas consecuencias. Los órganos nacionales interpretan las disposiciones de la nueva Directiva y luego, una vez que la Directiva está en vigor, es posible plantear una cuestión prejudicial ante el TJUE y preguntar si se implementó correctamente en las leyes nacionales. El futuro mostrará cómo los Estados miembros implementaron las reglas de la Directiva y cómo las interpretaciones difieren entre sí. Sólo el tiempo dirá cómo funciona la implementación de la nueva Directiva.

4. Una vez realizadas todas estas consideraciones surge de manera natural la siguiente pregunta: ¿Logrará la Unión Europa armonizar mejor las normas fragmentadas vigentes en

los 28 Estados miembros y proteger eficazmente los derechos fundamentales con respecto a las actividades cada vez más invasivas de los Estados, así como de terceros Estados (por ejemplo, EE.UU.)? Para poder ofrecer una respuesta, es necesario analizar cuatro principios o puntos clave sobre la protección de la privacidad que los Estados deben tener presentes en el diseño de las medidas dirigidas a una mayor seguridad pública, para que esas sean proporcionadas a la amenaza y respetuosas con la normativa de protección de datos.

1) Los derechos y libertades son una prioridad. Especialmente en circunstancias de "emergencia" en que la amenaza de las acciones terroristas lleva a la opinión pública a demandar más medidas policiales y preventivas intensificándose así los instrumentos de control y protección. En tiempos de paz, sin embargo, las medidas legislativas se centran más en la protección de los derechos, imponiendo límites a las acciones de las fuerzas de seguridad pública. La necesidad de garantizar la seguridad de los ciudadanos, por un lado, y proteger sus derechos, por otro, oscilan entre ellos como un péndulo, que avanza hacia la protección de los derechos cuando las condiciones económicas y sociales son más estables o va en la dirección de una mayor atención a las cuestiones de seguridad, cuando las demandas de la población en este sentido son más decisivas. En todo caso lo que nunca puede tolerarse es que, incluso en presencia de amenazas graves, los derechos fundamentales reconocidos y garantizados puedan desaparecer ya que se afectaría así a la dignidad humana, que es uno de los grandes fundamentos sobre los que se asienta el Estado democrático y de Derecho.

Por eso, para combatir el terrorismo, se necesitan más recursos para los servicios de inteligencia, las fuerzas y cuerpos de seguridad, pero también más recursos para la educación y la cultura, así como la necesidad de una intensa coordinación entre los Estados de la UE. La privacidad se encuentra hoy a la vanguardia de los derechos y las libertades y permite su disfrute tal y como se reconoce en nuestras Constituciones y Tratados internacionales, lo que reafirma la centralidad de los derechos y libertades fundamentales, que encuentran justo en la seguridad y la lucha contra la delincuencia la necesidad de conciliar intereses sólo aparentemente en conflicto. Sin embargo, para permitir que nuestros principios e ideales se arraiguen y crezcan, debemos evitar las simplificaciones que contraponen la privacidad y la seguridad. Los derechos fundamentales son una parte esencial de un sistema jurídico democrático y ocupan una posición privilegiada dentro de él.

Como hemos planteado en esta investigación, las actividades de recopilación y análisis de datos permiten, de hecho, hoy en día un perfil de individuos y grupos sociales tan precisos como para poder predecir su comportamiento y guiar sus decisiones individuales y

colectivas. De esta manera, la libertad personal, entendida como exenta de cualquier control ilícito, conlleva el riesgo de que tales tratamientos, si no están adecuadamente regulados puedan perder sentido y de esta manera incidir negativamente en las demás libertades. El hecho mismo de que la protección de datos sea ahora un baluarte contra los controles ilegales que afectan nuestra libertad, muestra que la protección de datos ahora no sólo es un derecho individual, sino un interés general fundamental de la Unión Europea y los Estados miembros. Veíamos más arriba como la UE establece en sus Tratados que ésta se fundamenta en el respeto a los mismos. Esto da lugar a la prohibición de su infracción, salvo cuando esté justificado por razones de interés general y, en todo caso, la limitación ha de ser proporcional al interés general perseguido. Por lo tanto, más que un equilibrio entre los derechos en el sentido técnico, es necesario identificar la proporcionalidad de las medidas introducidas, con respecto a la protección necesaria del núcleo central del derecho de que se trate. En consecuencia, es imprescindible determinar los riesgos y amenazas a la seguridad que puedan justificar suficientemente las eventuales restricciones a los derechos fundamentales y en qué condiciones. Tampoco podemos negar que muchas veces la imposición de restricciones a los derechos es necesaria en la búsqueda de objetivos legítimos como la seguridad nacional y la seguridad pública.

En cuanto al derecho a la privacidad y el interés colectivo en la seguridad, es necesario medir su relación en términos de razonabilidad y proporcionalidad, siendo el límite del derecho ciertamente justificado de acuerdo con un interés colectivo, pero sin que pueda extenderse más allá del núcleo esencial del derecho. Sin embargo, hemos de analizar si la interferencia en los derechos fundamentales es "necesaria" y si es "proporcionada" al fin legítimo perseguido, y si los motivos invocados por las autoridades nacionales para justificarla son oportunos, es decir, si es posible recurrir a una medida alternativa que causaría menos daño al derecho fundamental en cuestión, para cumplir con el mismo objetivo.

2) El derecho a la privacidad, desde su construcción jurisprudencial se ha convertido en un derecho codificado, gracias a un diálogo virtuoso y constante, tanto a nivel nacional como supranacional, entre el juez y el legislador. De hecho, a nivel europeo, la gran importancia de las decisiones establecidas por el TEDH y el TJUE para proteger el derecho a la privacidad han sido determinantes, precisamente con respecto a medidas restrictivas justificadas por razones de seguridad y pese al contexto social y político favorable a un endurecimiento de las medidas prevención y control. Ambos Tribunales tienen un enfoque similar en cuanto a la necesidad de salvaguardar las medidas que interfieren con los derechos de las personas. Ya sea cuando se trate de proteger las relaciones entre los ciudadanos de la

UE frente a los Estados que desean utilizar sus datos, o ya sea cuando se realice una evaluación de las modalidades de conservación de los datos obtenidos por las autoridades públicas, la jurisprudencia de los Tribunales, que se ha definido en el curso de los años de forma cada vez más oportuna, se orienta claramente hacia la limitación de los espacios de intervención de las autoridades, protegiendo el núcleo esencial del derecho en cuestión. Además, interviene en este sentido casi con los instrumentos típicos de un tribunal constitucional, transformando cuestiones prejudiciales, que generalmente se usan para proporcionar interpretación del Derecho de la Unión o sobre la validez de un acto de la Unión, en juicios de mérito basados en parámetros contenidos en la CDFUE.

Es evidente que la lucha contra el terrorismo representa un objetivo de interés general, como afirma también la jurisprudencia supranacional, y por lo que no se cuestiona tanto la obtención y conservación de datos, como los tiempos de conservación y las modalidades de acceso a ellos. Los Tribunales han sido prudentes con las nuevas tecnologías que permiten mayores posibilidades para que las autoridades interfieran con la privacidad de las personas. Cuando los datos personales se procesan por medios automatizados, la protección debe ser más fuerte. Las normas y la jurisprudencia europeas impiden una obtención general e indiscriminada de datos, porque no es proporcionada a las necesidades de investigación y al núcleo esencial del derecho a la protección de datos y, por lo tanto, no puede justificarse en una sociedad democrática. En cambio, los Estados miembros pueden establecer obligaciones de obtención de datos para fines específicos únicamente con el fin de contraste en delitos graves, siempre que estén temporalmente limitados en proporción a las necesidades de investigación y se refieran únicamente a la información "estrictamente necesaria". Además, la adquisición de los datos debe, según el TJUE, estar sujeta a condiciones específicas, incluido el control por un juez o una autoridad independiente. La vigilancia nunca puede ser generalizada y masiva, pero, como afirma el TJUE en el reciente fallo *Tele2 Sverige*, debe basarse en requisitos específicos, es decir, abordar a los involucrados, en cierta medida, en actividades delictivas o limitarse a lugares específicos en los que las necesidades de investigación surgen siempre relacionadas con delitos graves y después de una delimitación temporal adecuada de la duración de la conservación.

Incluso cuando el péndulo oscila por el lado de la seguridad, de hecho, el sistema de "protección multinivel" de los derechos en Europa ha demostrado que tiene defensas para proteger el núcleo esencial e irreductible de los derechos fundamentales, con ambos Tribunales supranacionales que parecen contribuir a la construcción de las piezas de un verdadero sistema de garantías de derechos. Y eso es aún más importante porque la amenaza al terrorismo, aunque con métodos diferentes, persiste desde hace muchos años y, por lo

tanto, es necesario encontrar un equilibrio estable, aunque flexible, entre las políticas de seguridad y la prevención y protección de las libertades fundamentales en general y de la privacidad en particular.

3) Rememorando la máxima latina "necessitas non habet legem", incluso en el Estado de Derecho, una acción que normalmente se considera ilegal puede convertirse en legal según las circunstancias. Para evitar el riesgo de convertir en permanente el recurso a normas que tratan por definición circunstancias excepcionales, y que la excepción se convierta en la regla, las medidas excepcionales que prevén la limitación de los derechos fundamentales no pueden imponerse a ultranza, sino que deben contar con el consentimiento del Parlamento, con un límite de tiempo preciso y debe ser ejecutada al amparo de la ley. En todo caso, con la posibilidad, cuando sea motivada, de ampliarse con medidas atenuadas conforme la emergencia se desvanece.

La limitación y/o interferencia de los derechos fundamentales está justificada si se basa en una disposición de la legislación que sea precisa, accesible para las personas afectadas y sus efectos sean previsibles. El nivel de precisión que se requiere de la ley depende del asunto específicamente abordado. La legislación debe regir el alcance y la aplicación de las medidas que interfieren con la privacidad del individuo. La legislación no puede prever todas las eventualidades, pero debe contar con garantías mínimas contra abusos: "limitación objetiva de los datos tratados, que deben ser los únicos realmente necesarios para la consecución de los fines establecidos por la ley; respeto por los principios de finalidad, relevancia y minimización del uso de datos de identificación personal; tiempos y métodos de conservación de los datos para mantenerlos razonables y proporcionados a las necesidades de las investigaciones de los delitos más graves; seguimiento de los accesos de terceros con respecto de cada tipología de trato; procedimientos para la destrucción y para proteger la integridad y confidencialidad de los datos". El ciudadano debe poder confiar en que sus datos sean precisos, tratados de manera legal y divulgados sólo a los destinatarios autorizados. Debe ser capaz de arreglar posibles fallos en sus datos.

Los intereses de seguridad nacional pueden prevalecer sobre los individuales, pero un objetivo de interés general no justifica una medida de retención de datos indiscriminada y generalizada. Los datos retenidos deben tener al menos algún tipo de relación con la seguridad pública. La legislación nacional debe basarse en pruebas objetivas de sujetos determinados cuyos datos puedan revelar un vínculo con delitos graves y ayudar de alguna manera a combatir estos delitos o prevenir un riesgo para la seguridad pública. El imperio

de la ley sirve para evaluar la legitimidad de determinadas medidas adoptadas y para observar si en su ejecución se han respetado los requisitos legales.

4) Buscar una mayor cooperación "efectiva" internacional entre las autoridades: la interoperabilidad. En los últimos años, como se ha analizado a lo largo de la investigación, la creciente necesidad de seguridad vinculada a la amenaza terrorista ha llevado a la adopción de nuevas estrategias de lucha contra el terrorismo que han impulsado el fortalecimiento de la cooperación entre las estructuras de seguridad y la lucha contra la delincuencia, y la creciente recogida, almacenamiento y tratamiento de datos personales con fines de seguridad, policía y justicia. Todo esto ha hecho cada vez más evidente la necesidad de proporcionar instrumentos adicionales, especiales y específicos de protección de datos tratados para estos fines que son capaces de garantizar un nivel de protección más elevado de lo que sucede en la actualidad. Este nuevo desafío plantea un difícil equilibrio de exigencias contradictorias entre garantizar un alto nivel de seguridad y proteger el derecho de la privacidad de cada individuo, que ha sido y sigue siendo, sin duda, una cuestión ardua. Es evidente que el desarrollo de una fuerte y mejor cooperación en materia de seguridad y judicial, mientras que responde a las necesidades reales de la eficiencia de los sistemas de control y seguridad, debe tener en cuenta el respeto de la vida privada y la protección de los datos personales, fundamentos contenidos en la CDFUE (artículos 7 y 8) y en el Tratado de Lisboa. Las actividades de cooperación se basan en el intercambio de informaciones e implican el tratamiento de datos personales para la prevención y represión de los delitos. Sin embargo, una extensión progresiva del uso de tal información, originalmente sólo prevista para controlar la inmigración para fines policiales, son ya prácticas reales, que generan motivos de preocupación adicional, ya que también es posible recoger datos que puedan dar una información muy precisa sobre una persona, a partir de los datos biométricos. Las autoridades policiales no sólo tienen la oportunidad de aprovechar la información, sino también para crear archivos electrónicos que, a causa del desarrollo tecnológico, pueden acumular grandes cantidades de datos. Por consiguiente, se debe evitar el riesgo de uso indebido de estos datos, incluso si su recogida y almacenamiento son fundamentales para la prevención de delitos graves y para garantizar la seguridad.

Las dificultades para conseguir una "cooperación efectiva" entre los Estados miembros también dependen de las diferencias entre las legislaciones entre los Estados europeos, por no mencionar la dinámica de los servicios de inteligencia de no compartir con los demás las informaciones y los datos pertinentes con el fin de la seguridad pública. Esta es una verdadera paradoja, porque, por una parte, se proclama la importancia de la recogida y el

intercambio de datos e información para fortalecer la cooperación en materia de "seguridad" contra el terrorismo y otras formas peligrosas de la delincuencia y, por otro lado, no se intercambian, entre los Estados europeos, los datos que serían muy útiles para el fin de seguridad pública. Por esto, se podría decir, que no hay necesidad de nuevos instrumentos de cooperación, sino de operar de manera efectiva y con los instrumentos ya existentes. Una legislación uniforme de la UE permite una "cooperación efectiva" entre las autoridades públicas. Ya en 2005, el Programa de La Haya estableció prioridades para el ELSJ, y describió "el principio de disponibilidad como la posibilidad de que la autoridad pública de un Estado miembro obtenga información de otro Estado miembro". La legislación de la UE debería uniformarse en toda la Unión y el canal de Europol debería utilizarse sistemáticamente en los Estados miembros para crear una imagen de la delincuencia transfronteriza a escala de la UE.

En realidad, la tendencia actual en Europa es que las autoridades traten de recopilar más datos. Sin embargo, las autoridades ya tienen acceso a una gran cantidad de datos, pero el problema es que aún no hay suficientes recursos para analizarlos. La respuesta correcta no es recopilar aún más datos, por ejemplo, el ADN de todos en archivos policiales, sino que la medida debe ser proporcional ya que el ADN de personas inocentes no debe figurar en los archivos policiales. Se trata de encontrar el equilibrio adecuado. Cuando las autoridades piden más herramientas para recopilar datos personales, primero deben evaluarse las herramientas ya existentes, en cuanto a si son efectivas. Es muy importante que las autoridades policiales responsables de la investigación sean efectivas en el futuro y el intercambio de información sin problemas entre las autoridades es ahora más importante que nunca. Una actuación multidisciplinar en este ámbito resulta prioritaria ya que, por las características de este campo, se hace necesaria una mejor cooperación con los ingenieros y la informática para mantener un enfoque basado en los derechos humanos. Los encargados de formular políticas, las autoridades públicas, las empresas, los académicos, los técnicos, los programadores y las personas deben cooperar para que la información sea la adecuada.

En estos términos, la mejora de la seguridad no depende de la mayor cantidad de datos obtenidos y de la menor privacidad que se garantiza a los ciudadanos, sino de la capacidad de análisis e intercambio de datos que las autoridades públicas ya poseen. Por lo tanto, es urgente un nuevo enfoque integral para salvaguardar y mantener la seguridad sin comprometer los valores y las libertades fundamentales de la UE. Es clave el "intercambio efectivo" de información entre las autoridades policiales nacionales, y entre los Estados miembros y las agencias pertinentes de la UE. Los sistemas de información de la UE existentes para la gestión de fronteras y la seguridad interior tienen deficiencias en las

funcionalidades de la gestión de datos fragmentada de la UE entre los diferentes sistemas de información, como SIS II, VIS y Eurodac. "El objetivo principal es garantizar que las autoridades policiales, aduaneras y judiciales competentes cuenten sistemáticamente con la información necesaria para el desempeño de sus funciones, manteniendo al mismo tiempo un equilibrio con respecto a los derechos a la privacidad, la protección de datos y otros derechos fundamentales".

La interoperabilidad es la capacidad de los sistemas de información para intercambiar datos y permitir el intercambio de información. Este intercambio no debe comprometer las reglas necesariamente estrictas de acceso y uso garantizadas por el RGPD, la Directiva de Protección de Datos para Autoridades Policiales y de Justicia Penal, la CDFUE y todas las demás normas pertinentes. Cualquier solución integrada para la gestión de datos no debe afectar los principios de limitación de la finalidad, "protección de datos por diseño" o "protección de datos por defecto".

5. La última cuestión tratada al final de esta investigación, se refiere a si el RGPD y la Directiva de protección de datos sobre asuntos policiales garantizan la protección del derecho a la privacidad de las personas contra las actividades invasivas de los Estados miembros, cuestión que todavía no tiene una respuesta clara. En nuestra opinión, una obligación general de conservar datos puede ser compatible con el Derecho de la UE, siempre que la acción de los Estados miembros cumpla los siguientes requisitos: 1) la obligación de conservación de datos debe tener una base legislativa o reglamentaria que posea las características de accesibilidad, previsibilidad y protección adecuada contra la injerencia arbitraria; 2) la obligación de respetar la esencia del derecho al respeto de la vida privada y del derecho a la protección de los datos personales; 3) únicamente la lucha contra la delincuencia grave es un objetivo de interés general que puede justificar una obligación general de conservar los datos; 4) la obligación general de conservar los datos debe ser estrictamente necesaria para luchar contra la delincuencia grave; 5) la obligación general de conservar los datos debe ser proporcionada; 6) el control a cargo de los organismos nacionales de supervisión independiente y acceso a una reparación judicial efectiva. Esas obligaciones deben respetar las condiciones con respecto al acceso a los datos, al período de conservación y la protección y seguridad de los datos, a fin de limitar la injerencia con los derechos fundamentales a lo estrictamente necesario. Cuando la información fluye libremente a través de las fronteras nacionales, la única forma de proteger a las personas cuya información se está transmitiendo es uniformar la legislación entre los Estados

miembros. La cooperación fluida entre las autoridades policiales es importante: cuanto las autoridades nacionales más cooperan, tanto más mejora la seguridad de las personas.

A nuestro juicio resulta esencial que el legislador europeo otorgue una mayor importancia al criterio de proporcionalidad, especialmente con referencia a la nueva legislación europea. Por último, la atención del legislador europeo debería centrarse más en la lógica de que un aparato normativo capaz de ofrecer suficiente protección a los datos personales es decisivo tanto para garantizar la seguridad de los ciudadanos en un sentido objetivo como para fortalecer su percepción subjetiva y, por lo tanto, su confianza en la sociedad digital globalizada. El futuro del derecho a la privacidad dependerá, sobre todo, del cumplimiento de la nueva normativa vigente, especialmente con respecto a los métodos de obtención y tratamiento de datos, y de la redefinición de las políticas de seguridad. Podemos concluir que, hasta hoy, no se ha verificado una aplicación completa y homogénea de las disposiciones para un posible "*Bill of Rights*" de la privacidad que estaba al alcance del legislador europeo, representada por los artículos 7 y 8 de la CDFUE.

Finalmente, hay que responder al conflicto privacidad *vs*. seguridad, ¿es verdaderamente así? La realidad es que la seguridad y la privacidad son dos caras de la misma moneda, dos derechos que son iguales en igual medida para cada individuo y que, inevitablemente, el respeto de uno depende de la protección del otro. Podemos decir que se trata de dos dimensiones diferentes de protección de la identidad de la persona, dos derechos y dos libertades que compiten por cada ciudadano sin tener que enfrentarse a la alternativa de elegir a uno de los dos, renunciando al otro. La seguridad va de la mano de la privacidad, así como del disfrute de todos los derechos fundamentales que son patrimonio de nuestro tiempo. Fortalecer el nivel de seguridad de cada ciudadano también significa superar la idea de buscar un equilibrio o una compensación de valores: todos los derechos deben ser protegidos y respetados, pero no pueden existir "aislados". No hay privacidad sin seguridad; no hay libertad sin privacidad…no hay libertad sin seguridad.

BIBLIOGRAFÍA CONSULTADA

ACED FÉLEZ, Emilio (2004): *¿Seguridad, privacidad, confidencialidad?: el desafío de la protección de datos personales*, Montevideo, Uruguay, Goethe-Institut Montevideo, Ediciones Trilce, págs. 222.

- (2007): «Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 65-96.
- (2010a): «La protección de datos en la cooperación policial europea: de la Recomendación (87) 15 al principio de disponibilidad. Título IV. Disposiciones Sectoriales. Cap. I. Ficheros de Titularidad Pública. Artículos 22, 23.1 y 24.1», en TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, págs. 1350-1388. ISBN 978-84-470-3423-9.
- (2010b), «Principio de disponibilidad y protección de datos en el ámbito policial», en *Noticias Jurídicas*. Disponible en Internet: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4537-principio-de-disponibilidad-y-proteccion-de-datos-en-el-ambito-policial-/.

AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2014): *Manual de legislación europea en materia de la protección de datos*, Luxemburgo, págs. 218. Disponible en Internet: http://www.echr.coe.int/Documents/Handbook_data_protection_SPA.pdf.

ALBRECHT, Jan Philipp, LAURISTIN, Marju and JOUROVÁ, Věra (2016): «New data protection rules fit for our digital age», en *Fondation EURACTIV*, 14 apr. Disponible en Internet: http://www.euractiv.com/section/digital/opinion/new-data-protection-rules-fit-for-our-digital-age/.

ALBRECHT, Jan-Philipp, SCHREMS, Max (2016): «Privacy Shield: The new EU rules on transatlantic data sharing will not protect you», en *The Irish Times*, 12 de Julio. Disponible en Internet: http://www.irishtimes.com/opinion/privacy-shield-the-new-eu-rules-on-transatlantic-data-sharingwill-not-protect-you-1.2719018.

ALDECOA LUZÁRRAGA, Francisco y GUINEA LLORENTE, Mercedes (2008): «El rescate sustancial de la Constitución Europea a través del Tratado de Lisboa: la salida del laberinto», en *Documento de Trabajo*, Real Instituto Elcano, núm. 9, págs. 32.

- (2010): *La Europa que viene: el Tratado de Lisboa*, Madrid, Editorial Marcial Pons, págs. 411.

ALFONSO RAMOS, Ana María (2014): *Derecho a la privacidad versus seguridad del Estado: límites en la lucha contra el terrorismo*, Trabajo fin de grado, Madrid, Repositorio de la Universidad Pontificia Comillas, págs. 59.

ALMUZARA ALMAIDA, Cristina (coord.), COUDERT, Fanny, MARZO PORTERA, Ana, NAVALPOTRO, Yolanda (2007): *Estudio práctico sobre la protección de datos de carácter personal*, 2ª ed., Valladolid, Lex Nova, págs. 706. ISBN: 9788484064367.

ALONSO GARCIA, Ricardo (1989): *Derecho Comunitario, Derechos Nacionales y Derecho Común europeo*, Madrid, Editorial Civitas, págs. 322.

- (2010), «Lisboa y el Tribunal de Justicia de la Unión Europea», en *Papeles de Derecho Europeo e Integración Regional*, Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense, núm. 1, págs. 32 Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2013-11-07-lisboa%20y%20el%20derecho.pdf.

ALONSO GARCÍA, Ricardo, SARMIENTO, Daniel (2006): *La Carta de los Derechos Fundamentales de la Unión Europea: explicaciones, concordancias, jurisprudencia*, Madrid, Editorial Civitas, págs. 472.

ÁLVAREZ CARO, María y RECIO GAYO, Miguel (2015): «Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU. y la UE», en *Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense Facultad de*

Derecho, Papeles de Derecho Europeo e Integración Regional, núm. 25, págs. 26. Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2015-06-15-Binder218.pdf.

ÁLVAREZ CARO, María (2015), *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Madrid, Editorial Reus, págs. 144.

ÁLVAREZ HERNANDO, Javier (2011): *Guía práctica sobre Protección de Datos: cuestiones y formularios*, Lex Nova.

ÁLVAREZ RUBIO, Juan José (2006): «Libertad, seguridad y justicia en la nueva Europa», en DEL RÍO VILLAR, Susana (coord.), *Europa: el Estado de la Unión*, Navarra, Editorial Aranzadi, págs. 119-138. ISBN 84-8355-029-6.

ANDRÉS SÁENZ DE SANTA MARÍA, Paz (2007): «El Tratado de Lisboa: Comienza una nueva etapa para Europa», en *Diario La Ley*, núm. 6851. ISSN 1989-6913.

ANGUITA VILLANUEVA, Luis Antonio (2004): «La cultura en la Carta de los Derechos Fundamentales de la Unión Europea», en RUÍZ MIGUEL, Carlos (coord.), *Estudio sobre la Carta de los derechos fundamentales de la Unión Europea*, Santiago de Compostela, Universidad de Santiago de Compostela, págs. 83-116. ISBN 84-9750-276-0.

ANÍBARRO MARTÍNEZ, Esther M. (2016): *El espacio de libertad, seguridad y justicia en la Unión Europea: proyecto jurídico-político "In Fieri"*, Tesis Doctoral, Valladolid, Universidad de Valladolid Instituto de Estudios Europeos, págs. 625.

APAP, Joanna and CARRERA, Sergio (2003): «Maintaining Security sitian Borders: Towards a Permanent State of Emergency in the EU?», en *CEPS Policy Brief - Centre for European Policy Studies*, núm. 41, págs. 13. Disponible en Internet: https://www.ceps.eu/publications/maintaining-security-within-borders-towards-permanent-state-emergency-eu.

ARACELI MANGAS, Martin (dir.) (2008): *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA, págs. 934. Disponible en Internet: http://www.fbbva.es/TLFU/dat/DE_2008_carta_drechos_fundamentales.pdf.

ARENAS RAMIRO, Mónica (2006): *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, págs. 638. ISBN13:9788484566489.

- (2008): «La protección de datos personales en los países de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 16, págs. 113-168. ISSN 1696-6759. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3057994.

ARZOZ SANTIESTEBAN, Xabier (2009): «Artículo 8: derecho al respeto de la vida privada y familiar», en LASAGABASTER HERRARTE, Iñaki (dir.), *Convenio Europeo de Derechos Humanos. Comentario sistemático*, 2ª ed., Madrid, Civitas, págs. 949.

ASOCIACIÓN PRO DERECHOS HUMANOS DE ESPAÑA (2011): *La adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos: su impacto institucional sobre la política y la ciudadanía europea. Jornada de expertos*, Madrid, 21 de octubre de 2011, págs. 67. Disponible en Internet: http://web.archive.org/web/20130811204959/http://apdhe.org/quehacemos/documentos/Folleto_Adhesion_UE_APDHE.pdf.

ATWILL, Nicole (2010): «European Court of Human Rights; France: Registration in French National Sex Offender Database Does Not Violate Rights», en *The Library of Congress*, Washington. Disponible en Internet: http://www.loc.gov/law/foreign-news/article/european-court-of-human-rights-france-registration-in-french-national-sex-offender-database-does-not-violate-rights/.

AUS, Jonathan P. (2006): «Eurodac: A Solution Looking for a Problem?», en *European integration online papers (EIoP)*, núm. 10, págs. 1-26. Disponible en Internet: http://eiop.or.at/eiop/pdf/2006-006.pdf.

AZURMENDI, Ana (2015): «Por un "derecho al olvido" para los europeos: aportaciones jurisprudenciales de la Sentencia del TJUE del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional de 29.12.2014», en *UNED. Revista de Derecho Político*,

núm. 92, enero-abril, págs. 273-310. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/14428.

BAEVERSTROEM, Jan (2016): «Reactions To The EU-US Privacy Shield, The Successor To The Safe Harbour Agreement», en *European Parliamentary Research Service Blog*, april 18. Disponible en Internet: https://epthinktank.eu/2016/04/18/reactions-to-the-eu-us-privacy-shield-the-successor-to-the-safe-harbour-agreement/.

BAINBRIDGE, David I., PLATTEN, Nick (1996): *EC Data Protection Directive*, London, Butterworths, págs. 328.

BALAGUER CALLEJÓN, Francisco (2008): «El Tratado de Lisboa en el diván. Una reflexión sobre estatalidad, constitucionalidad y Unión Europea», en *Revista Española de Derecho Constitucional*, año 28, núm. 83, págs. 57-92. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2702876.

BALDUCCI ROMANO, Fabio (2015): «La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo», en *Rivista Italiana di Diritto Pubblico Comunitario*, anno XXV, fasc. 6, págs. 1618-1659. Disponible en Internet: https://art.torvergata.it/retrieve/handle/2108/184345/367266/Fabio%20Balducci%20Romano.pdf.

BALZACQ, Thierry (2008): «The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies», en *JCMS: Journal of Common Market Studies*, volume 46, issue 1, págs. 75–100. Disponible en Internet: http://citation.allacademic.com//meta/p_mla_apa_research_citation/2/5/3/9/3/pages253934/p253934-1.php.

BALZACQ, Thierry, BIGO, Didier, CARRERA, Sergio, GUILD, Elspeth (2006): «Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats», en *CEPS Working Document*, núm. 234, págs. 28 Disponible en Internet: https://www.ceps.eu/publications/security-and-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats.

BAR CENDÓN, Antonio (2007): «El Tratado de Prüm y la inmigración ilegal», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 235-273.

BARBIERI, Cristian (2017): «Terrorismo: l'arma dello scambio dei dati», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/2017/05/terrorismo-larma-dello-scambio-dei-dati/.

BARDUTZKY, Samo (2014): «The Timing of Dialogue: Slovenian Constitutional Court and the Data Retention Directive», en *Verfassungsblog*. Disponible en Internet: http://www.verfassungsblog.de/timing-dialogue-slovenian-constitutional-court-data-retention-directive/.

BARLETT, Enric R., BARDAJÍ, María Dolores (coords.) (2012): *La Declaración Universal de los Derechos Humanos cumple 60 años. Seminario Permanente de Derechos Humanos Antonio Marzal. XV Sesión*, J.M. Bosch Editor, págs. 168.

BASSINI, Marco, POLLICINO, Oreste (2015): «La Corte di giustizia demolisce il *safe harbor* e ridisegna i confini del diritto alla privacy in ambito transnazionale», en *Diritto24 - Il Sole 24 Ore*, 7 ottobre. Disponible en Internet: http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2015-10-07/la-corte-giustizia-demolisce-safe-harbor-e-ridisegna-confini-diritto-privacy-ambito-transnazionale-153618.php.

BASSU, Carla (2017), «I diritti umani e le nuove sfide della sicurezza», en *Relazione tenuta al convegno annuale interdisciplinare del Dipartimento di Giurisprudenza dell'Università di Milano – Bicocca dedicato a Sicurezza e libertà in tempo di terrorismo globale*, svoltosi il 12 e 13 dicembre 2016, págs. 16.

BENDER, David (2015): «The Judicial Redress Act: A Path to Nowhere», en *International Association of Privacy Professionals*, Dec. 17. Disponible en Internet: https://iapp.org/news/a/the-judicial-redress-act-a-path-to-nowhere/.

BENITO MARTÍN, Ruth (2017): «¿Qué es una evaluación de impacto en protección de datos?», en *Lefebvre - El Derecho*, 18.04.2017. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/Evaluacion-impacto-reglamento-proteccion-datos_11_1076305003.html.

BESTAGNO, Francesco (2015): «Validità e interpretazione degli atti dell'UE alla luce della Corte: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali», en *Il Diritto dell'Unione Europea*, fasc.1, págs. 21-51.

BIFULCO, Raffaele (2016): «La sentenza Schrems e la costruzione del diritto europeo della privacy», en *Giurisprudenza costituzionale*, núm. 1, págs. 289-307.

BIFULCO, Raffaele, CARTABIA, Marta, CELOTTO, Alfonso (a cura di) (2001), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, Il Mulino, págs. 400.

BIGNAMI, Francesca (2007a): «Privacy and Law Enforcement in the European Union: the Data Retention Directive», en *8 Chicago Journal of International Law*, págs. 233-255. Disponible en Internet: http://scholarship.law.duke.edu/faculty_scholarship/1602/.

- (2007b): «European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining», en *Boston College Law Review*, vol. 48, págs. 609-698. Disponible en Internet: http://scholarship.law.gwu.edu/faculty_publications/225/.
- (2015): «The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens», en *Study for the LIBE Committee*, European Parliament, págs. 36. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf.

BIGNAMI, Francesca, RESTA, Giorgio (2015): «Transatlantic Privacy Regulation: Conflict and Cooperation», en *Law and Contemporary Problems*, vol. 78, págs. 101-134. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705601.

BIGO, Didier, CARRERA, Sergio, GONZÁLEZ FUSTER, Gloria, *et ál*. (2011), *Towards a New EU Legal Framework for Data Protection and Privacy. Challenges, Principles and the Role of the European Parliament*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, págs. 157. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/453216/IPOL-LIBE_ET(2011)453216_EN.pdf.

BIGO, Didier, CARRERA, Sergio, HAYES, Ben, HERNANZ, Nicholas and JEANDESBOZ, Julien (2012): «Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An Evaluation of Current and Forthcoming Proposals», en *CEPS Paper in Liberty and Security in Europe*, núm. 52, págs. 97. Disponible en Internet: https://www.ceps.eu/publications/justice-and-home-affairs-databases-and-smart-borders-system-eu-external-borders.

BIGO, Didier, CARRERA, Sergio, HERNANZ, Nicholas, *et ál*. (2013): *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, October, págs. 80. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

BIN, Roberto (2006): «Democrazia e terrorismo», en *Relazione svolta al Collegio Ghisleri di Pavia il 25 ottobre 2006, Collana della Facoltà di Giurisprudenza di Pavia*, Cedam, págs. 11.

BINDER, Christina (2015): «El Tribunal Europeo de Derechos Humanos y el Derecho de los Tratados ¿Fragmentación o Unidad?», en *Anuario español de Derecho Internacional*, vol. 31, págs. 297-321. Traducción del Dr. iur. Henry Jiménez Guanipa. ISBN: 0212-0747. Disponible

en Internet: https://www.unav.edu/publicaciones/revistas/index.php/anuario-esp-dcho-internacional/article/viewFile/4623/3985.

BIRNHACK, Michael (2008): «The EU Data Protection Directive: An Engine of a Global Regime», en *Computer Law & Security Report*, vol. 24, núm. 6, págs. 1-23.

BLASI CASAGRAN, Cristina (2010): «La protección de los Derechos Fundamentales en el Tratado de Lisboa», en *Quaderns de treball*, Institut Universitari d'Estudis Europeus, núm. 51. Disponible en Internet: http://ddd.uab.cat/record/77369/.

- (2015): «Límites del derecho europeo de protección de datos en el control de fronteras de la UE», en *Revista CIDOB d'Afers Internacionals*, núm. 111, págs. 127-151. ISSN:1133-6595. Disponible en Internet: https://www.cidob.org/articulos/revista_cidob_d_afers_internacionals/111/limites_del_derecho_europeo_de_proteccion_de_datos_en_el_control_de_fronteras_de_la_ue/(language)/esl-ES.
- (2016a): «El Reglamento Europeo de Europol: Un nuevo marco jurídico para el intercambio de datos policiales en la UE», en *Revista General de Derecho Europeo*, núm. 40, págs. 202-221. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5692787.
- (2016b): *Global Data Protection in the Field of Law Enforcement: An EU perspective*, London; N.Y., Routledge, págs. 264.
- (2017): «Nuevo Régimen Jurídico para la Transferencia de Datos entre la UE y los Estados Unidos ¿Es compatible con la Normativa Europea de Protección de Datos?», en *Revista General de Derecho Europeo*, núm. 42, págs. 193-217. Disponible en Internet: https://www.researchgate.net/publication/317662622.

BLASI CASAGRAN, Cristina y ILLAMOLA DAUSÀ, Mariona (coord.) (2016): *El control de las agencias del Espacio de Libertad, Seguridad y Justicia. Contrapeso necesario a su autonomía*, Madrid, Editorial Marcial Pons, págs. 210.

BOEHM, Franziska (2012): «Information Sharing in the Area of Freedom, Security and Justice – Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems», en GUTWIRTH, Serge, LEENES, Ronald, DE HERT, Paul, POULLET, Yves (eds.), *European Data Protection: In Good Health?*, Dordrecht, Springer, págs. 143-183.

- (2015): «A comparison between US and EU data protection legislation for law enforcement purposes», en *Study for the LIBE Committee*, European Parliament, págs. 77. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf.

BOEHM, Franziska, COLE, Mark D. (2014): *Data Retention after the Judgement of the Court of Juistice of the European Union*, study was provided by The Greens/EFA Group in the European Parliament, Münster/Luxembourg, 30 june, págs. 107. Disponible en Internet: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

BONFANTI, Matteo E. (2011): «Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti», en *Diritti umani e diritto internazionale*, vol. 5, núm. 3, págs. 437-481.

BONINI, Emanuele (2017): «Troppi database europei e pochi soldi per la sicurezza delle reti, l'Ue vuole più cybersecurity», en *Eunews*. Disponible en Internet: http://www.eunews.it/2017/06/29/troppi-database-europei-e-pochi-soldi-per-la-sicurezza-delle-reti-lue-vuole-piu-cybersecurity/88978.

BONINI, Monica (2016): «Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea», en *Rivista Associazione Italiana Costituzionalisti*, núm. 3/2016, págs. 33.

BORELLI, Davide (2016): «La valutazione di adeguatezza nei trasferimenti transfrontalieri di dati personali tra nuovo Regolamento europeo e (pre)vigente Direttiva», en *Diritto Mercato*

Tecnologia, 10 Dicembre. Disponible en Internet: http://www.dimt.it/index.php/it/notizie/15688-la-.

BORGER, Julian (2013): «GCHQ and European spy agencies worked together on mass surveillance», en *The Guardian*, Fri 1 Nov 2013. Disponible en Internet: https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

BOSCH MOLINÉ, Alba (2014): «La dimensión exterior de Europol desde el punto de vista de la protección de datos. El caso del acuerdo TFTP», en *Institute of Audit & IT-Governance (IAITG)*, págs. 33. Disponible en Internet: http://www.iaitg.eu/mediapool/67/671026/data/20140407_abosch_Europol.pdf.

BOTTA, Marco, VIOLA DE AZEVEDO CUNHA, Mario (2010): «La protezione dei dati personali nelle Relazioni tra UE e USA, le negoziazioni sul trasferimento del PNR», en *Il diritto dell'informazione e dell'informatica*, anno XXVI, fasc. 2, págs. 315-341. Disponible en Internet: https://www.academia.edu/995300/La_protezione_dei_dati_personali_nelle_Relazioni_tra_UE_e_USA_le_negoziazioni_sul_trasferimento_del_PNR.

BOUAZZA ARIÑO, Omar (2010): «Notas de jurisprudencia del Tribunal Europeo de Derechos Humanos», en *Revista de Administración Pública*, núm. 183, Madrid, págs. 263-279. ISSN: 0034-7639. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=1&IDN=1265&IDA=35645.

BOURNE, Charles (2012): «Retention and disclosure of police caution data infringe Article 8», en *The UK Human Rights Blog*. Disponible en Internet: https://ukhumanrightsblog.com/2012/11/15/retention-and-disclosure-of-police-caution-data-infringe-article-8-charles-bourne/.

BOWCOTT, Owen (2015): «UK-US surveillance regime was unlawful 'for seven years'», en *The Guardian*, Fri 6 Feb 2015. Disponible en Internet: https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa.

- (2016): «MP calls for limit on UK surveillance powers as EU test case opens», en *The Guardian*, 12 April. Disponible en Internet: https://www.theguardian.com/world/2016/apr/12/mp-david-davis-calls-limit-uk-surveillance-powers-european-court-justice.

BOWDEN, Caspar (2013): *The U.S. surveillance programmes and their impact on EU citizens' fundamental rights*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, September, págs. 37. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf.

BOWLES, Fern (2015): «European and national parliamentarians divided on the EU "Smart Borders Package"?», en *FREE Group*. Disponible en Internet: https://free-group.eu/2015/03/06/european-and-national-parliamentarians-divided-on-the-eu-smart-borders-package-february-23/.

BOWMAN, John (2015): «Paris Attacks Bring "Police" Directive Negotiations Back Into Spotlight», en *International Association of Privacy Professionals*, Feb 6. Disponible en Internet: https://iapp.org/news/a/paris-attacks-bring-police-directive-negotiations-back-into-spotlight/.

BRADWELL, Peter (2013): «EU Commission caved to US demands to drop anti-PRISM privacy clause», en *Open Rights Group*, June 14. Disponible en Internet: https://www.openrightsgroup.org/blog/2013/how-the-eu-commission-caved-to-us-demands-to-water-down-its-privacy-law.

BRITO, Noemí y CARBAYO, Francisco Javier (2016): «Autoridades europeas de protección de datos: clave de salvaguarda de la privacidad», en *Red Seguridad*, 14/01/2016. Disponible en Internet: http://www.redseguridad.com/especialidades-tic/proteccion-de-datos/autoridades-europeas-de-proteccion-de-datos-clave-de-salvaguarda-de-la-privacidad.

BRU CUADRADA, Elisenda (2007): «La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad», en *III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas*, organizado por los Estudios de Derecho y Ciencias Políticas de la UOC, núm. 5, págs. 78-92. Disponible en Internet: http://www.uoc.edu/idp/5/dt/esp/bru.pdf.

BURGESS, Matt (2016): «UN warns UK's IP Bill 'undermines' the right to privacy», en *wired.com.uk*. Disponible en Internet: http://www.wired.co.uk/article/un-privacy-ip-bill-not-compliant-international-law.

BURTON, Cedric, DE BOEL, Laura, KUNER, Christopher, PATERAKI, Anna, CADIOT, Sarah and HOFFMAN, Sára G. (2016): «The Final European Union General Data Protection Regulation», en *Bloomberg Law: Privacy & Data Security*, February 12. Disponible en Internet: https://www.bna.com/final-european-union-n57982067329.

BUTTARELLI, Giovanni (1997): *Banche dati e tutela della riservatezza*, Milano, Giuffrè, 1997.

- (2015): «Privacy, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche», en *federalismi.it*, núm. 1/2015, págs. 11.

BYGRAVE, Lee A. (2004): «Privacy Protection in the Global context: A comparative Overview», en *Scandinavian Studies in Law*, vol. 47, págs. 319-348.

CAGGIANO, Giandonato (2007): «L'evoluzione dello Spazio di libertà, sicurezza e giustizia nella prospettiva di un'Unione basata sul diritto», en *Studi sull'integrazione europea*, núm. 2, págs. 335-374. Disponible en Internet: http://www.studisullintegrazioneeuropea.eu/Scarico/Rivista%20Studi%200207.pdf.

- (2018): «Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione», en *MediaLaws - Rivista di diritto dei media*, núm. 2/2018 giugno, págs. 64-81.

CALAFIORE, Ilaria Maria (2016): «Budapest è solo il più recente caso di una legislazione antiterrorismo accusata in tutto il mondo di essere eccessivamente invasiva o repressiva», en *Eurocomunicazione.com*. Disponible en Internet: http://www.eurocomunicazione.com/lungheria-nuovamente-nel-mirino-delle-istituzioni-la-legge-antiterrorismo-non-salvaguarda-i-diritti-dei-cittadini/.

CALIFANO, Licia (2013): «*Privacy e sicurezza*», en *Democrazia & Sicurezza - Democracy and Security Review*, Saggi, Università degli Studi "Roma Tre", anno III, núm. 3, págs. 51.

CALONGE VELÁZQUEZ, Antonio (dir.) (2017), *Derecho Básico de la Unión Europea*, 2ª edición, Granada, Editorial Comares, págs. 216.

CALZOLAIO, Simone (2017): «Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679», en *federalismi.it*, núm. 24, págs. 21. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35361.

CÁMARA VILLAR, Gregorio (2007): «La garantía de los derechos fundamentales afectados por la Convención de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 97-118.

CANALES GIL, Álvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis, ORTUÑO SIERRA, Mercedes (coords.) (2006): *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Valencia, Tirant lo Blanch, págs. 350.

CANNATACI, Joseph A. (2013): «Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector», en *European Journal of Law and Technology*, vol. 4, núm. 2, págs. 35.

CANNATACI, Joseph A. and CARUANA, Mireille M. (2013): *Report: Recommendation R (87) 15 – Twenty–five years down the line*, Council of Europe, 25th September, págs. 172. Disponible en Internet: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf.

CANNATACI, Joseph A. and MIFSUD-BONNICI, Jeanne Pia (2005): «Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty», en *Information & Communications Technology Law*, vol. 14, issue 1, págs. 5-15.

CAREY, Peter (2015): *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press, págs. 864.

CARMONA BERMEJO, Julieta (2013): «Instituciones de apoyo a la Cooperación: Red Judicial Europea, Eurojust, Europol, Interpol, Magistrados de Enlace, IberRed», en CARMONA RUANO, Miguel, GONZÁLEZ VEGA, Ignacio U., MORENO CATENA, Víctor (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 943-997.

CARMONA CONTRERAS, Ana (2016): «El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales», en *Revista Española de Derecho Constitucional*, núm. 107, págs. 13-40. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5634735.

CARRASCOSA GONZÁLEZ, Javier (1997): «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, págs. 509-539. Disponible en Internet: http://www.academia.edu/11583471/Circulaci%C3%B3n_internacional_de_datos_personales_informatizados_y_la_Directiva_95_46_CE.

CARRERA MARISCAL, Andrea (2016): «Lo que debe saber sobre el Escudo de Privacidad entre la Unión Europea y los Estados Unidos», en *International Association of Privacy Professionals*, sep. 22. Disponible en Internet: https://iapp.org/news/a/lo-que-debe-saber-sobre-el-escudo-de-privacidad-entre-la-union-europea-y-los-estados-unidos.

CARRERA, Sergio y GEYER, Florian (2008): «El Tratado de Lisboa y un Espacio de Libertad, Seguridad y Justicia: Excepcionalismo y Fragmentación en la Unión Europea», en *Revista de Derecho Comunitario Europeo*, núm. 29, págs. 133-162. ISSN 1138-4026. Disponible en Internet: https://recyt.fecyt.es//index.php/RDCE/article/view/46494.

CARRERA, Sergio, DE SOMER, Marie and PETKOVA, Bilyana (2012): «The Court of Justice of the European Union as a Fundamental Rights Tribunal Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice», en *CEPS Paper in Liberty and Security in Europe*, núm. 49, págs. 29. ISBN: 978-94-6138-222-1. Disponible en Internet: http://aei.pitt.edu/36443/1/No_49_Carrera_et_al__ECJ_as_Fundamental_Rights_Tribunal2-2.pdf.

CARRILLO SALCEDO, Juan Antonio (2001): «Notas sobre el significado político y jurídico de la Carta de los Derechos Fundamentales de la Unión Europea», en *Revista de Derecho Comunitario Europeo*, núm. 9, págs. 7-26.

- (2004): *El Convenio Europeo de Derechos Humanos*, Madrid, Tecnos, págs. 160. ISBN: 9788430939374.

CARTABIA, Marta (2007): «L'ora dei diritti fondamentali nell'Unione Europea», en CARTABIA, Marta (a cura di), *I diritti in azione. Universalità e pluralismo dei diritti fondamentali nelle Corti europee*, Bologna, Il Mulino, págs. 13-66.

- (2011): «I 'nuovi' diritti», en *Atti del Convegno del CESEN "Diritto della Unione Europea e status delle confessioni religiose"*, Roma, Istituto L. Sturzo, 8-9 ottobre 2010, págs. 17. Disponible en Internet: http://www.olir.it/areetematiche/166/documents/cartabia_relazione_2010_roma_cesen.pdf.
- (2014): «La tutela multilivello dei diritti fondamentali. Evoluzioni della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona», en *Incontro trilaterale tra le Corti costituzionali italiana, portoghese e spagnola*, Santiago de Compostela, 16-18 ottobre 2014, págs. 21. Disponible en Internet: http://docplayer.it/1121975-La-tutela-multilivello-dei-diritti-fondamentali.html.

CASTELLANETA, Marina (2017): «Trasferimento dei codici di prenotazione: Lussemburgo boccia il progetto di accordo UE-Canada», en *marinacastellaneta.it*, luglio 28. Disponible en

Internet: http://www.marinacastellaneta.it/blog/trasferimento-dei-codici-di-prenotazione-lussemburgo-boccia-il-progetto-di-accordo-ue-canada.html.

CASTILLEJO MANZANARES, Raquel (2013): «Espacio Schengen», en CARMONA RUANO, Miguel, GONZÁLEZ VEGA, Ignacio U., MORENO CATENA, Víctor (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 267-319. Disponible en Internet: https://e-archivo.uc3m.es/handle/10016/18330.

CASTRONOVO, Carlo (2007): «La persona», en CASTRONOVO, Carlo, MAZZAMUTO, Salvatore (a cura di), *Manuale di diritto privato europeo*, Milano, Giuffrè, vol. 1, págs. 304.

CATALINA BENAVENTE, María Ángeles (2016): «La Directiva Europea (UE) 2016/681, de 27 de abril de 2016, relativa a la utilización de los datos por en la lucha contra el terrorismo y la delincuencia grave», en *Diario La Ley*, núm. 8801, 12 de julio.

CAVOUKIAN, Ann (2010): «Privacy by design: the definitive workshop. A foreword», en *Identity in the Information Society*, vol. 3, issue 2, págs. 247-251. Disponible en Internet: https://link.springer.com/article/10.1007/s12394-010-0062-y.

- (2011): «Privacy by Design. Strong Privacy Protection - Now, and Well into the Future», *A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners*, 2011, págs. 35. Disponible en Internet: https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf.

CIAMPI, Stefano (2009): «Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea», en PERONI, Francesco, GIALUZ, Mitja (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT, págs. 34-100. Disponible en Internet: https://www.openstarts.units.it/dspace/handle/10077/3350.

CIENFUEGOS MATEO, Manuel (2014): «La cuestión prejudicial comunitaria (Artículo 267 del Tratado de Funcionamiento de la Unión Europea)», en *Miami-Florida European Union Center of Excellence*, vol. 14, núm. 1, February, págs. 21. Disponible en Internet: http://aei.pitt.edu/63608/1/Cienfuegos_PrejudicialComunitariaEU_rev.pdf.

CIRILLO Gianpiero Paolo (2004): *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Padova, Cedam, 2004, págs. 296.

CLARKE, Roger (2009): «Privacy impact assessment: Its origins and development», en *Computer Law & Security Review*, vol. 25. Disponible en Internet: http://www.rogerclarke.com/DV/PIAHist-08.html.

CLARO QUINTÁNS, Irene (2003): «El sistema "Eurodac" y la identificación de los solicitantes de asilo en la Unión Europea», en DE TOMÁS MORALES, María Susana, HELLER DEL RIEGO, Christine y VAQUERO LAFUENTE, María Esther (coord.), *El día de Europa: las transformaciones de la Unión Europea: la ampliación y la convención europea: actas de las II jornadas en conmemoración del Día de Europa de la Universidad Pontificia Comillas de Madrid*, Madrid, Universidad Pontificia Comillas, 8 y 9 de mayo de 2003, págs. 215-228.

CODUTI, Daniele (2015): «Europol e ruolo dei parlamenti (nazionali ed europeo): quali prospettive dopo il Trattato di Lisbona?», en *Diritto Pubblico Europeo Rassegna online*, luglio, págs. 23. ISSN: 2421-0528. Disponible en Internet: http://www.edizioniesi.it/dperonline/data/uploads/articoli/coduti-europol.pdf.

COGLIEVINA Stella (2013): *Diritto antidiscriminatorio e religione. Uguaglianza, diversità e libertà religiosa in Italia, Francia e Regno Unito*, Libellula Edizioni, págs. 280.

COLCELLI, Valentina (2014): «La protezione dei dati personali. Profili ricostruttivi tra mercato interno e ordinamento nazionale», en *Diritto e Processo*, págs. 411-468. ISSN: 1722-1110. Disponible en Internet: http://docplayer.it/3217576-Valentina-colcelli-1.html.

COLE, David and FABBRINI, Federico (2015): «Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders», en *Forthcoming in International Journal of Constitutional Law; iCourts Working Paper Series n. 33*. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657514.

COLIVER, Sandra (2012): «National Security and the Right to Information», en *Right2INFO.org*, págs. 14. Disponible en Internet: https://www.opensocietyfoundations.org/sites/default/files/coliver-nsp-pace-20121220.pdf.

COLOMER HERNANDEZ, Ignacio (2015): *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Pamplona, Aranzadi, págs. 851. ISBN: 978-84-9059-917-4.

CONDE ORTIZ, Concepción (2005): *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Cádiz, Dykinson, págs. 116.

CONFORTI, Benedetto (2015): «Francia, lo stato di emergenza e lo stato di diritto», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/articolo.asp?ID=3262.

CONOLLY, Chris (2013): «EU/US Safe Harbour - Effectiveness of the Framework in relation to National Security Surveillance», en *Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens"*, Strasburgo, págs. 8.

COPPEL, Philip (2014): *Information Rights: Law and Practice*, 4ª ed., Oxford, Hart Publishing, págs. 1444. ISBN: 9781782251903.

CÓRDOBA CASTROVERDE, Diego (2014): «El "derecho al olvido" tras la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014», en *Revista de Jurisprudencia*, núm. 1, octubre. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/derecho_al_olvido-proteccion_de_datos_11_765430009.html.

CORTÉS MARTÍN, José Manuel (2010): «Jurisprudencia del Tribunal de Justicia de la Unión Europea. Septiembre–Diciembre 2009», en *Revista de Derecho Comunitario Europeo*, año 14, núm. 35, págs. 257-322. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3233868.

CORTESE, Bernardo (2013): «La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona», en *Il Diritto dell'Unione Europea*, núm. 2, págs. 313-335.

COSTAMAGNA, Francesco (2010): «Banche dati del Dna e lotta contro il crimine: quale tutela per i diritti fondamentali in Europa?», en *ISPI - Policy Brief*, núm. 197, págs. 10. Disponible en Internet: http://www.ispionline.it/it/documents/PB_197_2010.pdf.

COTINO HUESO, Lorenzo (2015): «El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal"», en *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, págs. 391-433. Disponible en Internet: http://documentostics.com/component/option,com_docman/task,doc_view/gid,1541/.

CRESPI, Serena (2015a): «Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati», en *Rivista Italiana di Diritto Pubblico Comunitario*, anno XXV, fasc. 3-4, págs. 818-842. ISSN: 1121-404X. Disponible en Internet: https://boa.unimib.it/retrieve/handle/10281/91952/135261/Datipersonali_Rivdirpubbcomunitario.pdf.

- (2015b): «La tutela dei dati personali UE a seguito della sentenza Schrems», en *Eurojus Centro di Eccellenza Jean Monnet presso l'Università degli Studi di Milano*. Disponible en Internet: http://www.eurojus.it/la-tutela-dei-dati-personali-ue-a-seguito-della-sentenza-schrems/.
- (2016): «La nuova proposta di decisione di adeguatezza della Commissione europea riguardo agli Usa: lo scudo UE/USA per la privacy», en *Eurojus Centro di Eccellenza Jean Monnet presso l'Università degli Studi di Milano*. Disponible en Internet: http://rivista.eurojus.it/la-nuova-proposta-di-decisione-di-adeguatezza-della-commissione-europea-riguardo-agli-usa-lo-scudo-ueusa-per-la-privacy/.

CRIADO GÁMEZ, Juan Manuel (2011): «La inadmisibilidad de la cuestión prejudicial prevista en el artículo 267 del Tratado de Funcionamiento de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 24, mayo, págs. 7-34. ISSN: 1696-6759. Disponible en Internet:

http://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1215245063566/_/1284174418863/Redaccion.

CRUZ VILLALÓN, Pedro (2017): «El valor de posición de la carta de derechos fundamentales en la comunión constitucional europea», en *UNED. Teoría y Realidad Constitucional*, núm. 39, págs. 85-101. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19146.

CHESTER, Jeff (2014): «CDD Files Complaint on U.S./EU Safe Harbour for Data Privacy at FTC/Filing Reveals Failure of U.S. Agreement to Protect European Privacy», en *Centre for Digital Democracy*.

CHICHARRO LÁZARO, Alicia (2015): «La transcendencia práctica del caso Facebook en relación con la transferencia masiva de datos personales desde la Unión Europea a Estados Unidos», en MATEOS MARTÍN, Concha, HERRERO GUTIÉRREZ, Francisco Javier (coords.), *La pantalla insomne*, Cuadernos Artesanos de Comunicación, núm. 90, págs. 1857-1884. Disponible en Internet: http://www.revistalatinacs.org/15SLCS/libro-colectivo-2015.html.

D'AMATO, Anthony (2010): «Human Rights as Part of Customary International Law: A Plea for Change of Paradigms», en *Faculty Working Papers*, paper 88, págs. 47-98. Disponible en Internet: http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/88.

D'ATENA, Antonio (2010): «La Constitución oculta de Europa (antes y después de Lisboa)», en *Revista de Derecho Constitucional Europeo*, año 7, núm. 13. Disponible en Internet: http://www.ugr.es/~redce/REDCE13/articulos/01DAtena.htm.

DAVARA RODRÍGUEZ, Miguel Ángel (1998): *La protección de datos en Europa: principios, derechos y procedimientos*, Madrid, Grupo Asnef-Equifax, págs. 204.

DE HERT, Paul (2015): «The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?», en *Utrecht Journal of International and European Law*, vol. 31, núm. 80. Disponible en Internet: https://utrechtjournal.org/articles/10.5334/ujiel.cz/.

DE HERT, Paul and BELLANOVA, Rocco (2009): «Data Protection in the Area of Freedom, Security and Justice: A System Still to be Fully Developed?», en *Briefing Paper*, Study requested by the European Parliament, Directorate General Internal Policies of the Union, Policy Department C, Citizens' Rights and Constitutional Affairs, Brussels, PE 410.692, págs. 23. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/note/join/2009/410692/IPOL-LIBE_NT(2009)410692_EN.pdf.

DE HERT, Paul and GUTWIRTH, Serge (2003): «Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies», en *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), págs. 111-162.

- (2006): «Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power», en CLAES, Erik and others (eds.), *Privacy and the Criminal Law*, Antwerp/Oxford, Intersentia, págs. 61-104. ISBN: 90 5095 545 2. Disponible en Internet: http://works.bepress.com/serge_gutwirth/5/.
- (2009): «Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action», en GUTWIRTH Serge and others (eds.), *Reinventing Data Protection?*, Springer Netherlands, págs. 3-44.

DE HERT, Paul and PAPAKONSTANTINOU, Vagelis (2009): «The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for», en *Computer Law and Security Review*, núm. 25, págs. 403–414. Disponible en Internet: http://www.vub.ac.be/LSTS/pub/Dehert/270.pdf.

- (2014a): «The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition», en *Computer Law & Security Review*, vol. 30, issue 6, págs. 633-642.
- (2014b): *The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area*, European Parliament - Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, Brussels, pág. 7. p. 40. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510001/IPOL_STU(2014)510001_EN.pdf.
- (2015): «Repeating the Mistakes of the Past will do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling», en *New Journal of European Criminal Law*, vol. 6, núm. 2, págs. 160-165.
- (2016): «The New Police and Criminal Justice Data Protection Directive: A First Analysis», en *New Journal of European Criminal Law*, vol. 7, issue 1, págs. 7-19. Disponible en Internet: http://journals.sagepub.com/doi/abs/10.1177/2032284416007001O2.

DE HERT, Paul, PAPAKONSTANTINOU, Vagelis and RIEHLE, Cornelia (2008), «Data protection in the Third Pillar: Cautious pessimism», en Martin MAIK, (ed.), *Crime Rights and the EU: The Future of the Police and Judicial Cooperation*, London, Justice, págs. 121-194. Disponible en Internet: http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf.

DE LLANO Pablo (2018): «Una consultora que trabajó para Trump manipuló datos de 50 millones de usuarios de Facebook», en *ElPaís.com*, 18 mar 2018. Disponible en Internet: https://elpais.com/internacional/2018/03/17/estados_unidos/1521308795_755101.html.

DE MINICO, Giovanna (2015): «Le libertà fondamentali in tempo di ordinario terrorismo», en *Federalismi.it*, núm. 10. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29517.

DE PRADA, Pilar Eirene (2015): «Privacidad en la era digital: El caso Zakharov», en *Rights International Spain*. Disponible en Internet: http://www.rightsinternationalspain.org/es/blog/92/privacidad-en-la-era-digital:-el-caso-zakharov.

DE TERWANGNE, Cécile (2014): «The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data», en *International Review of Law, Computers & Technology*, vol. 28, issue 2, págs. 118-130.

DE VRIES, Katja, BELLANOVA, Rocco & DE HERT, Paul (2010): «Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention», en *CEPS 'Liberty and Security in Europe'*, págs. 12. Disponible en Internet: https://www.ceps.eu/publications/proportionality-overrides-unlimited-surveillance.

DECLI, Federico, MARANDO, Gabriella (2009): «Le banche dati dell'Unione europea istituite per finalità di sicurezza e giustizia», en PERONI, Francesco, GIALUZ, Mitja (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT - Edizioni Università di Trieste, págs. 101-138. Disponible en Internet: http://www.openstarts.units.it/dspace/handle/10077/3351.

DEL MORAL TORRES, Anselmo (2010): «La cooperación policial en la Unión Europea: propuesta de un modelo europeo de inteligencia criminal», en *Análisis del Real Instituto Elcano (ARI)*, núm. 50. Disponible en Internet: http://www.realinstitutoelcano.org/wps/portal/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOKNg318fEKcHX1NTZz9QgKNXI0NDSBAvyDbUREAbg0Kqw!!/?WCM_GLOBAL_CONTEXT=/wps/wcm/connect/elcano/elcano_es/zonas_es/ari50-2010.

DEL NINNO, Alessandro (2015): «Invalidità della Decisione Safe Harbour per il trasferimento dei dati verso gli USA: l'impatto pratico sulla esportazione dei dati personali», en *Diritto e Giustizia*. Disponible en Internet: http://www.dirittoegiustizia.it/news/17/0000075868/Invalidita_della_Decisione_Safe_Harbour

_per_il_trasferimento_dei_dati_verso_gli_USA_l_impatto_pratico_sulla_esportazione_dei_dati_personali.html.

DESIMONE, Christian (2010): «Pitting Karlsruhe against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive», en *German Law Journal*, vol. 11, núm. 3, págs. 291–318. Disponible en Internet: http://www.germanlawjournal.com/volume-11-no-03/.

DI FRANCESCO MAESA, Costanza (2016): «Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)», en *Rivista Eurojus*. Disponible en Internet: http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/.

DI MARTINO, Alessandra (2005): «La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela», en PANUNZIO, Sergio P. (a cura di), *I diritti fondamentali e le corti in Europa*, Napoli, Jovene, págs. 365-482.

DI MINCO, Sandro (2012): «Commento all'art. 16 del TFUE», en CURTI GIALDINO, Carlo (dir.), *Codice dell'Unione Europea Operativo. TUE e TFUE commentati articolo per articolo*, Napoli, Edizioni Giuridiche Simone, págs. 2560.

DÍAZ DÍAZ, Efrén (2016): «The new European Union General Regulation on Data Protection and the legal consequences for institutions», en *Church, Communication and Culture*, 1:1, págs. 206-239, Disponible en Internet: https://doi.org/10.1080/23753234.2016.1240912.

- (2017): «La nueva LOPD: un paso para la adaptación legal a la nueva realidad social y digital», en *Lefebvre - El Derecho*, 23.11.2017. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/LOPD-adaptacion-realidad-social-digital_11_1161430002.html.

DÍAZ FERNÁNDEZ, Antonio M. (2012): «Evolución de la cooperación europea en inteligencia», en *Varia Historia*, Belo Horizonte, vol. 28, núm. 47, págs. 163-185. Disponible en Internet: http://www.scielo.br/pdf/vh/v28n47/08.pdf.

DÍAZ, Antonio M., REVENGA SÁNCHEZ, Miguel, JAIME JIMÉNEZ, Óscar y MARTÍNEZ MARTÍNEZ, Rafael (2005): «Marco teórico para el análisis de la cooperación europea en materia de inteligencia», en *VIII Congreso de la Asociación de Ciencia Política y de la Administración*, Madrid, págs. 24-31. Disponible en Internet: http://www.aecpa.es/uploads/files/congresos/congreso_07/area03/GT09/DIAZ-Antonio.pdf.

DIETRICH PLAZA, Cristina (2007): «El Tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 31-64.

DIEZ DE VELASCO, Manuel (2010): *Las organizaciones internacionales*, 16ª ed., Madrid, Tecnos, págs. 952.

DÍEZ-HOCHLEITNER, Javier (2013): «El derecho a la última palabra: ¿Tribunales constitucionales o Tribunal de Justicia de la Unión?», en *Instituto de Derecho Europeo e Integración Regional (IDEIR) Universidad Complutense Facultad de Derecho*, Papeles de Derecho Europeo e Integración Regional, núm. 17, págs. 38. ISSN: 2172-8542. Disponible en Internet: https://www.ucm.es/data/cont/docs/595-2013-11-07-el%20derecho%20a%20la%20%C3%BAltima%20palabra.pdf.

DIGGELMANN, Oliver, and CLEIS, Maria Nicole (2014): «How the Right to Privacy Became a Human Right», en *Human Rights Law Review*, vol. 14, págs. 441-458.

DONNINI, Francesco Maria (2017): *L'evoluzione della protezione dei dati personali tra tecnologia, sicurezza nazionale e diritti fondamentali*, Tesi di Laurea magistrale a ciclo unico, Università LUISS Guido Carli, págs. 268. Disponible en Internet: http://tesi.eprints.luiss.it/19180/.

E.L. (2016): «The new transatlantic data "Privacy Shield», en *The Economist*, feb 2nd. Disponible en Internet: http://www.economist.com/blogs/economist-explains/2016/02/economist-explains-2.

ERDOS, David (2015): «European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps» (September 1, 2015). A revised version of this paper is in the Journal of Law and Society (Winter 2016 Forthcoming); en *University of Cambridge Faculty of Law Research Paper*, núm. 30, págs. 31. Disponible en Internet: https://ssrn.com/abstract=2611583 or http://dx.doi.org/10.2139/ssrn.2611583.

ESQUINAS VALVERDE, Patricia (2010): *Protección de datos personales en la Policía Europea*, Valencia, Tirant lo Blanch, págs. 163.

ESSERS, Loek (2014): «Austrian court axes data retention law following EU high court ruling», en *Network World*, Jun 27. Disponible en Internet: http://www.networkworld.com/article/2401522/austrian-court-axes-data-retention-law-following-eu-high-court-ruling.html.

ESTADELLA YUSTE, Olga (1995): *La protección de la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, págs. 160.

ETXEBERRIA GURIDI, José Francisco (2009): «Principio de disponibilidad y protección de datos personales: a la búsqueda del necesario equilibrio en el espacio judicial penal europeo», en *Eguzkilore*, San Sebastián, núm. 23, págs. 351-366. Disponible en Internet http://www.ehu.eus/documents/1736829/2176697/26+Etxeberria.pdf.

EU-LISA (2014a): *Annual Activity Report 2013*, Luxembourg, Publications Office of the European Union, págs. 44. Disponible en Internet: http://www.eulisa.europa.eu/Publications/Corporate/ELAA13001ENC.pdf.

- (2014b): *eu-LISA in Action. IT in the service of a more open and secure Europe*, Luxembourg, Publications Office, págs. 16. Disponible en Internet: http://www.eulisa.europa.eu/Publications/Information%20Material/EL0214892ENC.pdf.
- (2015): *Informe anual de actividades consolidado de la eu-LISA*, 2016-009 REV 1, págs. 109. Disponible en Internet: https://www.eulisa.europa.eu/Publications/Documents/AAR2015/EU-LISA_2016_00040000_ES_TRA.pdf.

EUROPEAN CIVIL LIBERTIES NETWORK (2009): *Declaración del ECLN sobre el Programa de Estocolmo de la UE: Oponerse a las prácticas estatales autoritarias y crear una Europa democrática*, 15 de abril de 2009. Disponible en Internet: https://stockholm.noblogs.org/post/2009/04/15/declaraci-n-del-ecln-acerca-del-programa-de-estocolmo-de-la-ue/.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2010): *Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 56. Disponible en Internet: http://fra.europa.eu/en/publication/2010/data-protection-european-union-role-national-data-protection-authorities.

- (2011a): *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 72. Disponible en Internet: http://fra.europa.eu/en/publication/2011/access-justice-europe-overview-challenges-and-opportunities.
- (2011b): *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final)*, FRA Opinion - 1/2011, Vienna, 14 June 2011, págs. 23. Disponible en Internet: http://fra.europa.eu/en/opinion/2011/fra-opinion-proposal-passenger-name-record-pnr-directive.
- (2015): *Fundamental rights implications of the obligation to provide fingerprints for Eurodac*, Vienna, Publications Office, págs. 12. Disponible en Internet:

http://fra.europa.eu/en/publication/2015/fundamental-rights-implications-obligation-provide-fingerprints-eurodac.

- (2018): *Handbook on European data protection law 2018 edition*, Luxembourg, Publications Office of the European Union, April 2018, págs. 402.

FABBRINI, Federico (2015): «Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States», en *Harvard Human Rights Journal*, vol. 28, págs. 65-95. Disponible en Internet: http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf.

FALKVINGE, Rick (2016): «German studies eight years ago show that surveillance brings horrible self-censorship. Why is this news to the US now?», en *privateinternetaccess.com*, Mar 30. Disponible en Internet: https://www.privateinternetaccess.com/blog/2016/03/germans-studies-eight-years-ago-show-surveillance-brings-horrible-self-censorship-news-us-now/.

FALLETTA, Pietro (2015): «La Corte di Giustizia, ancora una volta, contro le multinazionali del Web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14)», en *federalismi.it*, núm. 24, págs. 11. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=31041.

FAVERO, Luca (2013): *La dimensione esterna della tutela dei dati personali nel diritto dell'unione europea*, Tesis Doctoral, Bologna, Alma Mater Studiorum - Università di Bologna, Dottorato di Ricerca in Diritto dell'Unione Europea, Ciclo XXV, págs. 179.

FERNÁNDEZ HERNÁNDEZ, Carlos (2016): «Las autoridades europeas publican nuevas directrices para la aplicación del Reglamento Europeo de Protección de datos», en *Diario La Ley*, 19-12-2016.

FERNÁNDEZ RODRÍGUEZ, José Julio (2016), «Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente», en *Revista Española de Derecho Constitucional*, núm. 108, págs. 93-122. Disponible en Internet: https://recyt.fecyt.es//index.php/REDCons/article/view/54343.

FERNÁNDEZ ROZAS, José Carlos (2004): «El Espacio de Libertad, Seguridad y Justicia consolidado por la Constitución Europea», en *Revista Juridica Española La Ley*, 4, D-195, págs. 1867-1881. Disponible en Internet: http://eprints.ucm.es/6870/1/EL_ESPACIO_DE_LIBERTAD%2C_SEGURIDAD_Y_JUSTICIA__CONSOLIDADO.pdf.

FERNÁNDEZ, Carlos B. (2017a): «¿Qué enmiendas deben introducirse en la propuesta de Reglamento europeo sobre ePrivacidad?», en *Diario La Ley*, 2-6-2017.

- (2017b): «El Parlamento Europeo avanza en la tramitación del Reglamento de E-Privacy con las primeras propuestas de modificación», en *Diario La Ley*, 14-6-2017.
- (2017c): «El Reino Unido adapta su normativa sobre protección de datos al Reglamento europeo», en *Diario La Ley*, 21-8-2017.
- (2018): «El Reglamento de e-Privacy precisa y complementa al RGPD, pero plantea muchos problemas prácticos», en *Diario La Ley*, Wolters Kluwer, 31-1-2018.

FERNÁNDEZ-LASQUETTY, Javier y BELLO, Martín (2017): «La legislación europea no permite una normativa nacional que recopile datos de tráfico y localización de manera indiscriminada. Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, Tele2 Sverige (C-203/15 y C-698/15)», en *Anuario ELZABURU de jurisprudencia europea en propiedad industrial e intelectual*, págs. 139-141. Disponible en Internet: http://www.elzaburu.es/en/document-centre/search-news-items?op=viewcms&id2=-3005116.

FERRARIS, Valeria (2017): «Eurodac e i limiti della legge: quando il diritto alla protezione dei dati personali non esiste», en *Diritto, Immigrazione e Cittadinanza*, núm. 2, págs. 16. Disponible en Internet: https://www.dirittoimmigrazionecittadinanza.it/archivio-saggi-commenti/saggi/fascicolo-2017-n-2/128-eurodac-e-i-limiti-della-legge-quando-il-diritto-alla-protezione-dei-dati-personali-non-esiste.

FERRER MARTÍN DE VIDALES, Covadonga (2008): «Los parlamentos nacionales en la Unión Europea tras el Tratado de Lisboa», en *Jean Monnet/Robert Schuman Paper Series*, vol. 8, núm.

16, págs. 33. Disponible en Internet: http://aei.pitt.edu/8907/1/deVidalesEUparliamentosLong08edi.pdf.

FINOCCHIARO, Giusella (2014): «Il diritto all'oblio nel quadro dei diritti della personalità», in *Il Diritto dell'informazione e dell'informatica*, anno XXIX, fasc. 4-5, págs. 591-604. Disponible en Internet: http://www.blogstudiolegalefinocchiaro.it/wp-content/uploads/2014/11/Giusella-Finocchiaro.pdf.

- (2016): «La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems», en RESTA, Giorgio, ZENO-ZENCOVICH, Vincenzo, *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, RomaTrE-Press, págs. 113-135. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/PTD.

FIORILLO, Valentina (2017): «Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali», en *federalismi.it*, núm. 15, págs. 24.

FLOR, Roberto (2014): «La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?», en *Diritto Penale Contemporaneo*, núm. 2, págs. 178-190. Disponible en Internet: http://www.penalecontemporaneo.it/foto/2396DPC_trim_2_2014.pdf#page=183&view=Fit.

FORNI, Lorena, VETTOR, Tiziana (a cura di) (2018): *Sicurezza e libertà in tempi di terrorismo globale*, G. Giappichelli Editore, mayo, págs. 304.

FREIXES SANJUÁN, Teresa (2005): «Derechos fundamentales en la Unión Europea. Evolución y prospectiva: la construcción de un espacio jurídico europeo de los derechos fundamentales», en *Revista de Derecho Constitucional Europeo*, año 2, núm. 4. Disponible en Internet: http://www.ugr.es/~redce/REDCE4/articulos/02freixes.htm.

FREIXES SANJUÁN, Teresa (2007): «Protección de datos y globalización. La Convención de Prüm», en *Revista de derecho constitucional europeo*, núm. 7, págs. 11-20. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2492884.

FUENTETAJA PASTOR, Jesús Ángel (2006): «Las agencias europeas de la cooperación policial y judicial», en *Revista de Derecho de la Unión Europea*, núm. 10, págs. 51-93. Disponible en Internet: http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:19805&dsID=AgEuCoPol.pdf.

FUERTES-PLANAS ALEIX, Cristina, SÁNCHEZ DE LA TORRE, Ángel (2016): *Principios jurídicos en la definición del derecho. Principios del Derecho II*, Dykinson, págs. 261.

GACITÚA ESPÓSITO, Alejandro Luis (2014): *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (en busca del equilibrio entre la libertad y la seguridad)*, Tesis Doctoral, Barcelona, Departamento de Ciencia Política y de Derecho Público Universidad Autónoma de Barcelona, mayo, págs. 440.

GALLI, Francesca (2016): «Ue e cooperazione giudiziaria: se l'Italia non attua Prüm», en *AffarInternazionali*. Disponible en Internet: http://www.affarinternazionali.it/2016/11/ue-e-cooperazione-giudiziaria-se-litalia-non-attua-prum/.

GAMBINO, Silvio (2010): «Jurisdicción y justicia entre Tratado de Lisboa, Convenio Europeo de Derechos Humanos y ordenamientos nacionales», en *Revista de Derecho Constitucional Europeo*, año 7, núm. 13. Disponible en Internet: http://www.ugr.es/~redce/REDCE13/articulos/04Gambino.htm.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2015): *Relazione 2015*, Roma, págs. 239.

- (2016a): *Relazione 2016*, Roma, págs. 236.
- (2016b): *La società sorvegliata. I nuovi confini della libertà*, Roma, Atti del convegno tenuto in occasione della Giornata europea della protezione dei dati personali 2016, págs. 184.
- (2017): *Relazione 2017*, Roma, págs. 245.

GARCÉS-MASCAREÑAS, Blanca (2015): «Por qué Dublín "no funciona"», en *notes internacionals CIDOB 135*. Disponible en Internet: https://www.cidob.org/publicaciones/serie_de_publicacion/notes_internacionals/n1_135_por_que_dublin_no_funciona/por_que_dublin_no_funciona.

GARCÍA ROCA, Francisco Javier (2007): «La muy discrecional doctrina del margen de apreciación nacional según el Tribunal Europeo de Derechos Humanos: soberanía e integración», en *UNED. Teoría y Realidad Constitucional*, núm. 20, págs. 117-143. ISSN: 1139-5583. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2520040.

GARCÍA SAN JOSÉ, Daniel I. (2001): *Los derechos y libertades fundamentales en la sociedad europea del siglo XXI: análisis de la interpretación y aplicación por el Tribunal Europeo de derechos humanos de la cláusula "necesario en una sociedad democrática"*, Sevilla, Universidad de Sevilla, págs. 218.

GARCÍA-BERRIO HERNÁNDEZ, Teresa (2003): *Informática y libertades. La protección de datos personales y su regulación en Francia y España*, Murcia, Universidad de Murcia, Servicio de Publicaciones, págs. 498.

GARCÍA-VALDECASAS Y FERNÁNDEZ, Rafael, CARPI BADÍA, José María (2004): «El Tribunal de Justicia de la Unión Europea. Algunas consideraciones respecto a su papel en el marco de la construcción europea», en *Revista Jurídica de Castilla y León*, núm. 3, págs. 13-48. Disponible en Internet: http://portaljuridico.lexnova.es/revista-castilla-leon/documento/760/6737/el-tribunal-de-justicia-de-la-union-europea-algunas-consideraciones-respecto-a-su-papel-en-el-marco.

GARRIDO RODRÍGUEZ, Pedro (2012): *Inmigración y diversidad cultural en España. Un análisis histórico desde la perspectiva de los derechos humanos*, Salamanca, Ediciones Universidad de Salamanca, págs. 690.

GARRIGA DOMÍNGUEZ, Ana (2016), *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, págs. 270.

GARZÓN CLARIANA, Gregorio (1981): «La protección de los datos personales y la función normativa del Consejo de Europa», en *Revista de Instituciones Europeas*, vol. 8, núm. 1, págs. 9-25 Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/fondo-historico?IDR=5&IDN=713&IDA=28020.

GELLMAN, Robert (2014): «Foreigners' privacy rights in the US: Little more than a gesture», en *Privacy Laws & Business*, August, issue 130, págs. 7-9. Disponible en Internet: https://www.bobgellman.com/rg-docs/rg-PL&B-PA-Gesture-14.pdf.

GERADTS, Zeno, SOMMER, Peter (eds.) (2008): *D6.7c: Forensic Profiling*, Future of Identity in the Information Society (FIDIS), págs. 67. Disponible en Internet: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.7c.Forensic_Profiling.pdf.

GIANNITI, Pasquale (a cura di) (2015): *La CEDU e il ruolo delle Corti: globalizzazione e promozione delle libertà fondamentali*, Bologna, Zanichelli, XLVII, págs. 2032. ISBN: 9788808421104.

GIBBS, Samuel and BOWCOTT, Owen (2016): «'Robust' deal reached to preserve privacy of EU-US data sharing», en *The Guardian*, tuesday 2 february. Disponible en Internet: http://www.theguardian.com/technology/2016/feb/02/robust-deal-reached-to-preserve-privacy-of-eu-us-data-sharing.

GOBIERNO DE ESPAÑA (2018): *Plan Anual Normativo 2018*, pags. 140.

GÓMEZ SÁNCHEZ, Yolanda (2007): «Los datos genéticos en el Tratado de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 137-165.

GÓMEZ, Rosario G., SAHUQUILLO, María R. (2013): «Los colosos de la Red se alían contra la nueva ley de privacidad de la UE», en *El País*, Madrid, 24 Feb. Disponible en Internet: http://sociedad.elpais.com/sociedad/2013/02/24/actualidad/1361744770_097775.html.

GONZÁLEZ FUSTER, Gloria (2009): «TEDH - Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Artículo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas», en *Revista de Derecho Comunitario Europeo*, núm. 33, págs. 619-633. ISSN: 1138-4026. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=679&IDA=27523.

- (2014a): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer International Publishing, vol. 16, págs. 274. ISBN 978-3-319-05022-5.
- (2014b): «La privacidad en Europa ¿Un debate cada vez más fundamental o cada vez menos?», en *Revista TELOS (Cuadernos de Comunicación e Innovación)*, Madrid, Fundación Telefónica, págs. 9. ISSN: 0213-084X. Disponible en Internet: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2014042309560003&idioma=es.

GONZÁLEZ MONJE, Alicia (2017): «Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto», en *Revista Europea de Derechos Fundamentales*, núm. 29, págs. 267-294 Disponible en Internet: http://journals.sfu.ca/redf/index.php/redf/article/view/224.

GONZÁLEZ PASCUAL, María Isabel (2014): «EL TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland», en *Revista de Derecho Comunitario Europeo*, núm. 49, Madrid, septiembre/diciembre, págs. 943-971. ISSN: 1138-4026. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=1336&IDA=37257.

GONZÁLEZ-CASTELL, Adán Carrizo (2008): «Instrumentos de asistencia policial en la Unión Europea: de Schengen a las estructuras orgánicas de cooperación policial», en BUJOSA VADELL, Lorenzo M., CALVO SÁNCHEZ, María del Carmen (coord.), *Hacia un verdadero Espacio Judicial Europeo*, 1ª ed., Granada, Comares, págs. 159-195.

GRAZIANI, Chiara (2018): «PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali», en *DPCE Online*, vol. 33, núm. 4, págs. 959-966. Disponible en Internet: http://www.dpceonline.it/index.php/dpceonline/article/view/474.

GREEN, Damon (2011): «Safe Harbor-a framework that works», en *International Data Privacy Law*, vol. 1, issue 3. Disponible en Internet: https://doi.org/10.1093/idpl/ipr010.

GREENLEAF, Graham (2013a): «Modernising data protection Convention 108: A safe basis for a global privacy treaty?», en *Computer Law & Security Review*, vol. 29, págs. 12. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262296.

- (2013b): «Uruguay starts Convention 108's global journey with accession», en *Privacy Laws & Business International Report*, issue 122, págs. 7. Disponible en Internet: http://ssrn.com/abstract=2280121.
- (2016): «Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives», en *142 Privacy Laws & Business International Report*, 14-17; *UNSW Law Research Paper*, núm. 17-3, págs. 9. Disponible en Internet: https://ssrn.com/abstract=2892947.

GUAGENTI, Antonella (2016): *La nuova disciplina in materia di protezione dei dati personali*, Tesi di laurea magistrale, Università di Pisa, Dipartimento di Giurisprudenza, págs. 232. Disponible en Internet: https://etd.adm.unipi.it/t/etd-05182016-171637/.

GUELLA, Flavio (2017): «Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali», en *DPCE on line*, vol. 30, núm. 2, págs. 349-357.

GUERRERO PICÓ, María del Carmen (2005): «El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea», en *Revista de Derecho Constitucional Europeo*, núm. 4, págs. 293-332. ISSN: 1697-7890. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=1972267.

- (2006): *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, Thomson-Civitas.

GUILD, Elspeth, CARRERA, Sergio (2014): «The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive», en *CEPS Liberty and Security in Europe Papers*, núm. 65, may 29, págs. 17. Disponible en Internet: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2445901.

GUTIÉRREZ DEL CASTILLO, Víctor Luis y LÓPEZ JARA, Manuel (2017): *El desarrollo y consolidación del Espacio de Libertad, Seguridad y Justicia de la UE. La implementación del Programa de Estocolmo*, Madrid, Editorial Tecnos, págs. 301. ISBN: 978-84-309-7070-4.

GUTIÉRREZ ZARZA, Ángeles (2017): «Terrorismo yihadista, crisis migratorias, fronteras, prueba electrónica, encriptado, referéndum y otras palabras clave del espacio LSJ en 2016», en *Diario La Ley*, Sección Tribuna, Editorial Wolters Kluwer, núm. 8904. Disponible en Internet: http://diariolaley.laley.es/home/DT0000240761/20170111/Terrorismo-yihadista-crisis-migratorias-fronteras-prueba-electronica-encriptado-.

GUTWIRTH, Serge, LEENES, Ronald, DE HERT, Paul (eds.) (2015): *Reforming European Data Protection Law*, Dordrecht, Springer Netherlands, págs. 406. ISSN: 2352-1929.

GUZMÁN GARCÍA, María de los Ángeles (2013): *El derecho fundamental a la protección de datos personales en México. Análisis desde la influencia del ordenamiento jurídico español*, Madrid, Tesis inédita de la Universidad Complutense de Madrid, Facultad de Derecho, Departamento de Derecho Constitucional, págs. 388.

HANNUM, Hurst (1996): «The Status of the Universal Declaration of Human Rights in National and International Law», en *The Georgia Journal of International and Comparative Law*, vol. 25, págs. 287-397.

HARRIS, David, O'BOYLE, Michael, BATES, Edward and BUCKLEY, Carla (2014): *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights*, 3ª ed., Oxford, Oxford University Press, págs. 1080. ISBN: 9780199606399.

HASBROUCK, Edward (2016): «The limits of the US Judicial Redress Act» en *Privacy Laws & Business*, issue 140, april, págs. 21-23. Disponible en Internet: https://papersplease.org/wp/wp-content/uploads/2016/02/JudicialRedressAct.pdf.

HAYES, Ben (2004): «Statewatch analysis. From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained», en *Statewatch Report*, London, págs. 46. Disponible en Internet: http://www.statewatch.org/news/2005/may/analysis-sisII.pdf.

HELISKOSKI, Joni (2008): «Small arms and light weapons within the Union's pillar structure: An analysis of Article 47 of the EU Treaty», en *European Law Review*, vol. 33, núm. 6, págs. 898-912.

HEREDERO HIGUERAS, Manuel (1994): «La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal», en VV.AA., *Informática judicial y protección de datos*, Victoria-Gasteiz, Departamento de Justicia del Gobierno Vasco.

- (1997): *La directiva comunitaria de protección de los datos de carácter personal: comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Pamplona, Aranzadi, págs. 375.
- (2006): «La protección de los datos de interés policial y judicial en la Unión Europea. De Schengen a Prüm», en *Revista Jurídica de Navarra*, núm. 42, págs. 119-142. Disponible en Internet: http://www.navarra.es/home_es/Navarra/Derecho+navarro/Revista+Juridica+de+Navarra/Sumarios/sumario42.htm [consulta: 01 de febrero de 2016].

HERMIDA DEL LLANO, Cristina (2005): *Los derechos fundamentales en la Unión Europea*, Barcelona, Anthropos Editorial, págs. 348. ISBN: 9788476587508.

HERRÁN ORTIZ, Ana Isabel (1998): *La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson, págs. 395. ISBN: 84-8155-409-X.

- (2002): *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*, Madrid, Editorial Dykinson, págs. 388.
- (2003): *El derecho a la protección de datos personales en la sociedad de la información*, Bilbao, Universidad de Deusto, Instituto de Derechos Humanos, Cuadernos Deusto de Derechos

Humanos, núm. 26, págs. 93. Disponible en Internet: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf.

HERRERO DE LA FUENTE, Alberto A. (coord.) (2003): *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*, Fundación Rei Afonso Henriques, págs. 267.

HIJMANS, Hielke (2016): *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer International Publishing, págs. 604.

HIJMANS, Hielke and SCIROCCO, Alfonso (2009): «Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?», en *Common Market Law Review*, vol. 46, issue 5, págs. 1485-1525. Disponible en Internet: http://www.ivir.nl/publicaties/download/1711.pdf.

HILDEBRANDT, Mireille (2009): «Who is Profiling Who? Invisible Visibility», en GUTWIRTH, Serge, POULLET, Yves, DE HERT, Paul and others (eds.), *Reinventing Data Protection?*, Dordrecht, Springer, págs. 239-252. Disponible en Internet: https://www.researchgate.net/publication/226541992_Who_is_Profiling_Who_Invisible_Visibility.

HUERTA, Pablo Pascual (2017): *La génesis del derecho fundamental a la protección de datos personales*, Tesis Doctoral, Madrid, Universidad Complutense de Madrid Facultad de Derecho Departamento de Derecho Constitucional, págs. 369.

HUSOVEC, Martin (2014): «First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU», en *The Center for Internet and Society*, 28 april. Disponible en Internet: http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court.

ILLAMOLA DAUSÀ, Mariona (2015): «EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE», en *Revista CIDOB d'Afers Internacionals*, núm. 111, págs. 105-126. Disponible en Internet: http://www.cidob.org/es/articulos/revista_cidob_d_afers_internacionals/111/eu_lisa_el_nuevo_modelo_de_gestion_operativa_de_las_distintas_bases_de_datos_de_la_ue.

ITALIANO, Ilenia (2015): *La protezione dei dati personali e il bilanciamento con altri diritti personali nel Diritto dell'Unione Europea*, Tesis Doctoral, Roma, Università degli Studi Roma Tre Scuola Dottorale Internazionale "Tullio Ascarelli" Diritto - Economia - Storia, Sezione "diritto europeo su base storico comparatistica", XVII° Ciclo, págs. 152.

JACOBS, James B., LARRAURI, Elena (2015): «Disclosure of nonconviction records may violate European Convention on Human Rights», en *Collateral Consequences Resource Center*. Disponible en Internet: http://ccresourcecenter.org/2015/01/30/criminal-record-privacy-according-european-court-human-rights/.

JAIME-JIMÉNEZ, Óscar, CASTRO MORAL, Lorenzo (2010): «La criminalidad organizada en la Unión Europea. Estado de la cuestión y respuestas institucionales», en *Revista CIDOB d'Afers Internacionals*, núm. 91, págs. 173-194. Disponible en Internet: http://www.raco.cat/index.php/revistacidob/article/viewFile/211125/280787.

JÄRVINEN, Heini (2014): «Denmark: Data Retention is here to stay despite the CJEU ruling», en *European Digital Rights (EDRi)*, 4 June. Disponible en Internet: https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling.

JÁUREGUI BERECIARTU, Gurutz y UGARTEMENDÍA ECEIZABARRENA, Juan Ignacio (2007): «Europa en el lecho de Procusto: de la Constitución Europea al Tratado de Lisboa», en *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkarian*, núm. 79, págs. 105-126. ISSN 0211-9560.

JIMÉNEZ GARCÍA, Francisco (2014): «La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa», en JORDÀ CAPITÁN, Eva R. y DE PRIEGO FERNÁNDEZ, Verónica (dirs.), *La protección y seguridad de la persona en internet. Aspectos sociales y jurídicos*, Madrid, Editorial Reus, págs. 208. ISBN: 978-84-290-1776-2.

JONES, Chris (2014): «Analysis 11 Years of Eurodac», en *Statewatch News Online*, págs. 17. Disponible en Internet: http://database.statewatch.org/article.asp?aid=33094.

JONSSON CORNELL, Anna, GOLDONI, Marco (eds.) (2017): *National and Regional Parliaments in the EU-Legislative Procedure Post-Lisbon. The Impact of the Early Warning Mechanism*, Hart Publishing, págs. 384.

KLIMAS, Tadas and VAIČIUKAITĖ, Jūratė (2008): «The Law of Recitals in European Community Legislation», en *ILSA Journal of International and Comparative Law*, vol. 15, págs. 33. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604.

KLITOU, Demetrius (2014): *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, T.M.C. Asser Press, págs. 338.

KOBRIN, Stephen J. (2004): «Safe Harbours are Hard to Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance», en *Review of International Studies*, núm. 30, págs. 111-131. Disponible en Internet: https://mgmt.wharton.upenn.edu/profile/1334/research.

KOKOTT, Juliane and SOBOTTA, Christoph (2013): «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», en *International Data Privacy Law*, vol. 3, núm. 4. Disponible en Internet: https://academic.oup.com/idpl/article/3/4/222/727206/The-distinction-between-privacy-and-data.

KORFF, Douwe (2002): *EC Study on Implementation of Data Protection Directive 95/46/EC*, REPORT on the findings of the study by Douwe Korff consultant to the European Commission, págs. 253. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667.

- (2004): «The legal framework: An analysis of the 'Constitutional' European approach to issues of data protection and law enforcement», en BROWN, Ian and KORFF, Douwe, *Privacy & Law Enforcement*, UK Information Commissioner study project.
- (2015): «EU-US Umbrella Data Protection Agreement: Detailed analysis by Douwe Korff», en *European Area of Freedom Security & Justice-FREE Group*, 14 October. Disponible en Internet: https://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/.

KOSTA, Eleni (2013): «The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection», en *SCRIPTed*, vol. 10, issue 3, october. Disponible en Internet: http://script-ed.org/?p=1163.

KUNER, Christopher (2007): *European Data Protection Law. Corporate Compliance and Regulation*, Second Edition, Oxford, Oxford University Press, págs. 592. ISBN: 9780199283859.

- (2012): «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law», en *Bloomberg BNA Privacy and Security Law Report*, págs. 1-15. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781.
- (2013): *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, págs. 312. ISBN: 9780199674619.

KUNER, Christopher, BYGRAVE, Lee and DOCKSEY, Christopher (2019): «Draft commentaries on 10 GDPR articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)», en *Commentary on the EU General Data Protection Regulation (GDPR)*, Forthcoming in 2019 from Oxford University Press, págs. 148.

LA RUE, Frank (2013): «Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión», Naciones Unidas, Asamblea General, A/HRC/23/40, 17 de abril de 2013, págs. 1-24.

LADENBURGER, Clemens (2008): «The Resources of European Security-Developing the EU Treaty Bases for Police Cooperation and Judicial Cooperation in Criminal Matters», en

European Review of Public Law, Esperia Publications Ltd, vol. 20, núm. 1, 2008, págs. 125-150.

LEFFI, Matteo (2017a): «L'Accordo PNR tra Canada e UE non prende il volo. Nota sul parere della Corte di giustizia europea a proposito del trasferimento dei dati del codice di prenotazione», en *media laws*. Disponible en Internet: http://www.medialaws.eu/laccordo-pnr-tra-canada-e-ue-non-prende-il-volo-nota-sul-parere-della-corte-di-giustizia-europea-a-proposito-del-trasferimento-dei-dati-del-codice-di-prenotazione/.

- (2017b): «I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE», en *Rivista di Diritti Comparati*, núm. 1, October 27, págs. 187-205. Disponible en Internet: http://www.dirittocomparati.it/wp-content/uploads/2017/11/Leffi8.pdf.

LESTER, Lord, PANNICK, Lord and HERBERG, Javan, (2009): *Human Rights Law and Practice*, London, Butterworth.

LEVIN, Avner and JO NICHOLSON, Mary (2005): «Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground», en *University of Ottawa Law & Technology Journal*, vol. 2, núm. 2, págs. 357-395.

LITTLE, Jonathon, PAEZ, Mauricio F., ROBERTSON, Elizabeth, *et*. *al*. (2016): «The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws», en *Jones Day Publications*, august. Disponible en Internet: http://www.jonesday.com/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws-08-11-2016/.

LÓPEZ AGUILAR, Juan Fernando (2017): «La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU», en *UNED. Teoría y Realidad Constitucional*, núm. 39, págs. 557-581. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19165.

LÓPEZ CALVO, José (2017a): «Las crecientes exigencias del consentimiento y el control institucional del clausulado en protección de datos», en *Diario La Ley Sección Ciberderecho*, Editorial Wolters Kluwer, núm. 10, 11 de septiembre.

- (2017b): *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin - Servicio de Propiedad, págs. 329.
- (2018): *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Madrid, Wolters Kluwer, págs. 850.

LÓPEZ CARBALLO, Daniel (2016): «A vueltas con las transferencias internacionales de datos: actualidad y seguridad jurídica», en *Actualidad Jurídica Aranzadi*, 22 de septiembre. Disponible en Internet: http://dlcarballo.com/wp-content/uploads/2016/09/AJA-922.pdf.

LÓPEZ GUERRA, Luis M. (2013): «El sistema europeo de protección de derechos humanos», en GALINDO, George Rodrigo Bandeira, URUEÑA, René, TORRES PÉREZ, Aida (coords.), *Protección multinivel de derechos humanos. Manual*, Barcelona, Red de Derechos Humanos y Educación Superior, págs. 165-186. ISBN: 978-84-697-0063-1. Disponible en Internet: http://e-archivo.uc3m.es/handle/10016/19770.

LÓPEZ PORTAS, M.ª Begoña (2015): «La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE», en *UNED. Revista de Derecho Político*, núm. 93, mayo-agosto, págs. 143-175. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/15140.

LÓPEZ-TORRES, Jonathan (2014): «Antecedentes internacionales en materia de privacidad y protección de datos personales», en *Ejil - EAFIT Journal of International Law*, [S.l.], v. 5, n. 2, págs. 103-117.

LUCARELLI, Alberto e PATRONI GRIFFI, Andrea (a cura di) (2009): *Dal Trattato costituzionale al Trattato di Lisbona: nuovi studi sulla Costituzione europea*, Napoli, Edizioni Scientifiche Italiane, págs. 526.

LUQUE GONZÁLEZ, José Manuel (2004): «Schengen. Un espacio de libertad, seguridad y justicia», en *Revista de derecho: División de Ciencias Jurídicas de la Universidad del Norte*,

núm. 21, págs. 139-149. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2347493.

LYNSKEY, Orla (2014): «Deconstructing data protection: the 'Added-value' of a right to data protection in the EU legal order», en *International and Comparative Law Quarterly*, núm. 63, vol. 3, págs. 569-597. ISSN: 0020-5893. Disponible en Internet: http://eprints.lse.ac.uk/57713/.

- (2015): *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, págs. 307.
- (2017): «Tele2 Sverige Ab and Watson et al: continuity and radical change», en *The European Law Blog*, january 12. Disponible en Internet: http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/.

MACDONALD, Raegan (2013): «Human Rights Day: EU's Data Protection Reform: restoring trust by reinforcing user rights», en *accessnow.org*, 10 december. Disponible en Internet: https://www.accessnow.org/human-rights-day-eus-data-protection-reform-restoring-trust-by-reinforcing/.

- (2015): «As Privacy Regulation moves to trialogue, Access warns of dangerous loopholes in Council text», en *accessnow.org*, 15 June. Disponible en Internet: https://www.accessnow.org/as-privacy-regulation-moves-to-trialogue-access-warns-of-dangerous-loopholes-in-council-text/.

MADISON, James (2009): «Federalist n. 51», en HAMILTON, Alexander, MADISON, James y JAY, John, *The Federalist Papers*, ed. Michael A. Genovese, Nueva York, Palgrave Macmillan, págs. 119-122.

MANGIAMELI, Stelio (2006): *L'ordinamento europeo. L'esercizio delle competenze*, vol. 2, Giuffrè Editore, págs. 622.

MANTELERO, Alessandro (2015): «Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo», en *Il Diritto dell'Informazione e dell'Informatica*, anno XXX, fasc. 4-5, págs. 887-908. Disponible en Internet: http://www.academia.edu/23759403/Il_trattamento_dati_nelle_imprese_nel_post_Safe_Harbour._Strategie_di_breve_medio_e_lungo_periodo.

- (2016): «From Safe Harbour to Privacy Shield. The "Medieval" sovereignty on personal data», en *Contratto e Impresa/Europa*, núm. 1. Disponible en Internet: https://www.researchgate.net/publication/303522873_From_Safe_Harbour_to_Privacy_Shield_The_Medieval_sovereignty_on_personal_data.

MARANDOLA, Antonella (2009): «Information sharing nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione», en PERONI, Francesco, GIALUZ, Mitja (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, EUT - Edizioni Università di Trieste, págs. 164-189. Disponible en Internet: https://www.openstarts.units.it/dspace/handle/10077/3352.

MARCHETTI, Gloria (2012): «I recenti passi avanti compiuti dall'Unione europea nella direzione di un'armonizzazione dei sistemi penali. Aspetti positivi, aspetti problematici e prospettive di riforma», en *Research Paper Centro Studi sul Federalismo*, págs. 28. Disponible en Internet: http://www.csfederalismo.it/attachments/article/834/CSF-RP_Marchetti_Ue_armonizzazione_sistemi_penali_Nov2012.pdf.

MARECOS GAMARRA, Adriana (2013): «El derecho a la autodeterminación informativa en España y Europa», en *Observatorio Iberoamericano de Protección de Datos*, 25 marzo. Disponible en Internet: https://oiprodat.wordpress.com/2013/03/25/el-derecho-a-la-autodeterminacion-informativa-en-espana-y-europa/ [Consulta: 10 de julio 2015].

MARICA, Andreea (2012): «El sistema de tratamiento de la información en EUROPOL», en *Institut de Ciències Polítiques i Socials (ICPS)*, WP núm. 309, págs. 30. Disponible en Internet: http://www.icps.cat/archivos/Workingpapers/wp309.pdf?noga=1.

MARQUENIE, Thomas (2017): «The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework», en *Computer Law & Security Review*, vol. 33, issue 3, June, págs. 324-340.

MARTÍN MARTÍNEZ, Magdalena M. (2010): «Terrorismo y derechos humanos en la Unión Europea y en el Consejo de Europa: ¿marco de referencia mundial?», en *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz 2009*, núm. 1, págs. 395-426. Disponible en Internet: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2009/2009_10.pdf.

- (2014): «Límites a la libre circulación de personas en la UE por razones de orden público, seguridad o salud pública en tiempos de crisis: una revaluación a la luz de la jurisprudencia del TJUE», en *Revista de Derecho Comunitario Europeo*, núm. 49, septiembre/diciembre, págs. 767-804. ISSN 1138-4026. Disponible en Internet: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=1336&IDA=37252.

MARTÍN Y PÉREZ DE NANCLARES, José (2007): «La posición del Parlamento Europeo en el espacio de libertad, seguridad y justicia», en BARBÉ, Esther, HERRANZ SURRALLÉS, Anna (eds.), *Política exterior y Parlamento Europeo: hacia el equilibrio entre eficacia y democracia*, págs. 67-83. ISBN 978-92-823-2183-6. Disponible en Internet: http://www.recercat.cat/bitstream/handle/2072/204360/7%20cap%205.pdf?sequence=7.

MARTÍN Y PÉREZ DE NANCLARES, José y URREA CORRES, Mariola (2010): *Tratado de Lisboa. Textos consolidados del tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea*, 2ª edición, Madrid, Marcial Pons y Real Instituto Elcano, págs. 395.

MARTÍNEZ MARTÍNEZ, Ricard (2007): «El derecho fundamental a la protección de datos: perspectivas», en *III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas*, organizado por los Estudios de Derecho y Ciencias Políticas de la UOC, núm. 5, págs. 47-61. Disponible en Internet: http://www.uoc.edu/idp/5/dt/esp/martinez.html.

MARTÍNEZ PÉREZ, Fernando y POZA CISNEROS, María (2013a): *El Principio de Disponibilidad: Antecedentes Penales y Convenio de Prüm*, 5ª edición, Madrid, Consejo General del Poder Judicial, págs. 98. Disponible en Internet: http://www5.poderjudicial.es/cvcp12-13/CVCP13-09-ES.pdf.

- (2013b): «El principio de Disponibilidad: antecedentes penales y Convenio de Prüm», en CARMONA RUANO, Miguel, GONZÁLEZ VEGA, Ignacio U., MORENO CATENA, Víctor (dir.), *Cooperación Judicial Penal en Europa*, Universidad Carlos III de Madrid. Instituto de Justicia y Litigación Alonso Martínez, Madrid, Editorial Dykinson, págs. 417-496.

MARTÍNEZ, Ricard (2015): «Safe Harbor: retos para el modelo europeo de la privacidad», en *Lefebvre – El Derecho*, 19.10.2015. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/Safe-Harbor-modelo-europeo-privacidad_11_874180003.html.

- (2016): «Desde un punto de vista jurídico la privacidad es un derecho cuya titularidad es irrenunciable», en *Lefebvre - El Derecho*, Madrid, 28.01.16. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/dia-europeo-proteccion-datos-privacidad-derecho-irrenunciable_14_912070001.html.

MARTOS, Natalia (2017): «Se acerca el 25 de mayo de 2018. ¿Está su empresa adaptada al nuevo Reglamento de Protección de Datos?», en *Diario La Ley*, núm. 9081, Sección Tribuna, 15 de noviembre de 2017, Editorial Wolters Kluwer.

MASSÉ, Estelle, STEPANOVICH, Amie, MITNICK, Drew (2016): «Activating the EU-US Privacy Shield: To protect privacy, we need reform, not rebranding», en *accessnow.org*, 4 february. Disponible en Internet: https://www.accessnow.org/activating-the-eu-us-privacy-shield/.

MASTRACCI, Marco (2017): «L'Accordo quadro tra USA e UE sul trasferimento dei dati personali per il contrasto della criminalità», en *La Comunità Internazionale*, vol. LXXII, núm. 1, págs. 37-57. Disponible en Internet: http://www.mpmlegal.it/public/pubblicazioni/5mastracci.pdf.

MASTROIANNI, Roberto (2009): «La tutela dei diritti fondamentali tra diritto comunitario e Costituzioni nazionali», en *Convegno Corte di Cassazione "La tutela dei diritti fondamentali*

tra Corte costituzionale, Corti europee e giudice nazionale", Roma, 21 gennaio 2009, págs. 42. Disponible en Internet: www.europeanrights.eu/public/commenti/relazione_Prof1._Mastroianni.doc.

MAYALI, Laurent and YOO, John (2016): «A Comparative Examination of Counter-Terrorism Law and Policy», en J*ournal of Korean Law*, vol. 16, págs. 91-144. Disponible en Internet: https://ssrn.com/abstract=2949078.

MAYOR GÓMEZ, Roberto (2016): «Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)», en *GABILEX*, núm. 6, junio, págs. 25. Disponible en Internet: http://www.castillalamancha.es/sites/default/files/documentos/pdf/20160709/revista_gabilex_no_6._autor_roberto_mayor_gomez.pdf.

MCNAMEE, Joe (2016): «Press Release: Vote on Data Protection and Passenger Name Record package», en *European Digital Rights (EDRi)*, 13 Apr 2016. Disponible en Internet: https://edri.org/press-release-data-protection-and-passenger-name-record-package-to-be-voted-on-tomorrow/.

MELCHIONNA, Silvia (2004): «I principi generali», en ACCIAI, Riccardo (a cura di), *Il diritto alla protezione dei dati personali*, Rimini, Maggioli Editore, 2004, págs. 29-66.

MENDEZ, Mario (2017): «Opinion 1/15: The Court of Justice Meets PNR Data (Again!)», en *European Papers*, vol. 2, núm. 3, págs. 803-818. Disponible en Internet: http://www.europeanpapers.eu/en/e-journal/opinion-1-15-court-of-justice-meets-pnr-data-again?utm_source=European+Papers+-+Newsletter&utm_campaign=64d3c64732-EP_Newsletter_2017_No_11&utm_medium=email&utm_term=0_8a90fc1b72-64d3c64732-121233561.

MENDOZA LOSANA, Ana I. (2015): «Transferencias internacionales de datos personales: Estados Unidos no es un puerto seguro, pero tampoco una isla inalcanzable», en *Centro de Estudios de Consumo (C.E.S.C.O.) Universidad de Castilla-La Mancha*, págs. 18. Disponible en Internet: http://blog.uclm.es/cesco/files/2015/10/Transferencias-internacionales-de-datos-personales_Estados-Unidos-no-es-un-puerto-seguro-pero-tampoco-una-isla-inalcanzable.pdf.

MEROLA, Faustoluigi (2016): «Decisione di Esecuzione (UE) 2016/1209 della Commissione del 12/07/2016. Disposizioni di attuazione per il sistema d'informazione Schengen di seconda generazione (SIS II)», en *AmbienteDiritto.it*, págs. 21. Disponible en Internet: https://www.ambientediritto.it/home/dottrina/decisione-di-esecuzione-ue-20161209-della-commissione-del-12072016.

MESEGUER, Marina (2016): «ThinThread, el programa secreto que podría haber evitado los atentados del 11S», en *LaVanguardia.com*, 11/09/2016. Disponible en Internet: http://www.lavanguardia.com/internacional/20160911/41223154746/thinthread-programa-secreto-evitado-atentados-11s.html.

MESSINA, Michele (2014): «La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità», en *Osservatorio sulla Corte di Giustizia dell'Unione europea*, núm. 2, págs. 396-401. Disponible en Internet: http://www.rivistaoidu.net/sites/default/files/Paragrafo%203_0.pdf.

MIGLIETTI, Lucia (2014): «Profili storico-comparativi del diritto alla privacy», en *Diritti Comparati*, December 4.

MILLÁN MORO, Lucía (2010): «El ordenamiento jurídico comunitario: del Tratado Constitucional al Tratado de Lisboa», en *Revista de Derecho Comunitario Europeo*, núm. 36, págs. 401-438. Disponible en Internet: http://www.cepc.gob.es/gl/publicaci%C3%B3ns/revistas/revistas-electronicas?IDR=4&IDN=1260&IDA=27881.

MILT, Kristiina (2019): «La protección de los datos personales», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales.

MINERO ALEJANDRE, Gemma (2017): «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», en *Anuario Jurídico y Económico Escurialense*, págs. 13-58. ISSN: 1133-3677.

MINISTERIO DE JUSTICIA (1992): *Recomendaciones y resoluciones del Comité de Ministros del Consejo de Europa en materia jurídica*, Madrid, págs. 574.

MODAFFERI, Francesco (2015): *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Roma, Lulu.com, págs. 374. ISBN: 9781326464059.

MONTELEONE, Shara (2007), «La disciplina del trattamento dei dati personali in Europa», en *Teutas Law & Technology*.

MONTES FERNÁNDEZ, Francisco José (2014): «El Consejo de Europa», en *Anuario Jurídico y Económico Escurialense*, núm. 47, págs. 57-92. ISSN: 1133-3677. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=4639615.

MONTI, Andrea (2016): «Privacy Shield: i nodi irrisolti (e irrisolvibili)», en *AgendaDigitale.eu*, 15 luglio. Disponible en Internet: http://www.agendadigitale.eu/egov/privacy-shield-i-nodi-irrisolti-e-irrisolvibili_2374.htm.

MORGAN, Richard, BOARDMAN, Ruth (2012): *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell, págs. 450.

MORINI, Claudia (2008): «La Convenzione di Prüm sulla cooperazione transfrontaliera specialmente in materia di lotta al terrorismo, al crimine transnazionale e all'immigrazione illegale», en *Studi sull'integrazione europea*, núm. 1, págs. 181-201. Disponible en Internet: http://www.studisullintegrazioneeuropea.eu/Scarico/Rivista%20Studi%200108.pdf.

MORTE GÓMEZ, Carmen y CANO PALOMARES, Guillem (2010): «La interpretación evolutiva y dinámica del Convenio Europeo de Derechos Humanos en la jurisprudencia reciente del Tribunal de Estrasburgo», en *Revista General de Derecho Constitucional*, núm. 10, págs. 31.

MOWBRAY, Alastair (2012): *Cases, Materials, and Commentary on the European Convention on Human Rights*, 2ª ed., Oxford, Oxford University Press, págs. 936. ISBN: 9780199577361.

MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis (2009): *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, págs. 184. ISBN: 978-84-613-3470-4.

MURRAY, Patrick J. (1997): «The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?», en *Fordham International Law Journal*, vol. 21, issue 3, págs. 932-1018. Disponible en Internet: http://ir.lawnet.fordham.edu/ilj/vol21/iss3/10/.

MUSSELLI, Lucia (2013): «Alcune prime considerazioni sui sistemi di scambio di informazioni nello spazio di libertà, sicurezza e giustizia: securitization, function creep e tutela dei diritti», en *Research Paper Centro Studi sul Federalismo*, págs. 23. Disponible en Internet: http://www.csfederalismo.it/attachments/article/832/CSF-RP_Musselli_Sistemi_di_scambio_di_informazioni_maggio2013.pdf.

NASCIMBENE, Bruno (2016): «La tutela dei diritti fondamentali nella giurisprudenza della Corte di giustizia», en *Convegno in occasione dei primi 25 anni della Rivista italiana di diritto pubblico comunitario, Diritto europeo e diritti amministrativo nazionale 25 anni dopo*, in data 11.11.2016. págs. 7. Disponible en Internet: http://rivista.eurojus.it/la-tutela-dei-diritti-fondamentali-nella-giurisprudenza-della-corte-di-giustizia/.

NEDERLANDS JURISTEN COMITÉ VOOR DE MENSENRECHTEN (2016): «La ley de escuchas telefónicas rusa es un "queso suizo" judicial, sentencia el Tribunal de Estrasburgo», en *Civil Liberties Union for Europe*, febrero 26. Disponible en Internet: http://www.liberties.eu/es/news/cedh-ve-ley-escuchas-telefonicas-rusas-como-un-queso-suizo-judicial.

NI AOLAIN, Fionnuala and GROSS, Oren (2001): «From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights», en *Human Rights Quarterly*, núm. 23, págs. 625-649. Disponible en Internet: http://uir.ulster.ac.uk/15678/.

NIELSEN, Nikolaj (2013): «MEPs copy-pasting amendments from US lobbyists», en *EUobserver*, Brussels, 12 Feb. Disponible en Internet: https://euobserver.com/justice/119028.
- (2016): «EU parliament passes grand data protection law», en *EUobserver*, Brussels, 14 Apr. Disponible en Internet: https://euobserver.com/justice/133060.

NINO, Michele (2015): «La Corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbour: la sentenza Schrems», en *SIDIBlog*, vol. 2. Disponible en Internet: http://www.sidiblog.org/2015/10/24/la-corte-di-giustizia-ue-dichiara-linvalidita-del-sistema-di-safe-harbour-la-sentenza-schrems/.

NOVAK, Petr y RAFFAELLI, Rosa (2017): «El Tratado de Lisboa», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo, págs. 5. Disponible en Internet: http://www.europarl.europa.eu/ftu/pdf/es/FTU_1.1.5.pdf.

O'BRIEN, Kevin J. (2013): «Silicon Valley Companies Lobbying Against Europe's Privacy Proposals», en *The New York Times*, Jan. 25. Disponible en Internet: http://www.nytimes.com/2013/01/26/technology/eu-privacy-proposal-lays-bare-differences-with-us.html?_r=0.

OHM, Paul (2010), «Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization», en *UCLA Law Review*, vol. 57, núm. 6, págs. 1701–1777. Disponible en Internet: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

OLESTI RAYO, Andreu (2008): «Las políticas de la Unión Europea relativas al control en las fronteras, asilo e inmigración», en *Revista de Derecho Constitucional Europeo*, núm. 10, págs. 13-48. ISSN 1697-7890. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=3013952.

ORAA, Jaime, GÓMEZ ISA, Felipe (1997): *La Declaración Universal de los Derechos Humanos. Un breve comentario en su 50 Aniversario*, Bilbao, Universidad de Deusto, págs. 90.

ORDÓÑEZ SOLÍS, David (2003): «El espacio judicial de libertad, seguridad y justicia en la Unión Europea», en *Revista de Estudios Políticos*, núm. 119, págs. 447-484. ISSN 0048-7694. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=496725.
- (2017): «Crónica de la jurisprudencia del Tribunal de Justicia de la Unión Europea», en *Cuadernos Europeos de* Deusto, núm. 56, págs. 207-250. Disponible en Internet: http://ced.revistas.deusto.es/article/view/1292.

OROFINO, Marco (2018): «Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione», en *MediaLaws - Rivista di diritto dei media*, núm. 2/2018 giugno, págs. 82-104.

ORTEGA GIMÉNEZ, Alfonso (2007): «Transferencia internacional de datos de carácter personal: U.E. vs. EE.UU.», en *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, vol. 1, núm. 2, marzo, págs. 210-219. ISSN: 1886-6611. Disponible en Internet: https://revistasocialesyjuridicas.files.wordpress.com/2010/09/02-tm-09.pdf.
- (2014a): «Algunas claves en las relaciones entre los EEUU y la UE sobre transferencias de datos de carácter personal. El acuerdo de Puerto Seguro», en *Revista TELOS (Cuadernos de Comunicación e Innovación)*, Madrid, núm. 97, febrero-mayo. Disponible en Internet: https://telos.fundaciontelefonica.com/seccion=1268&idioma=es_ES&id=2014042309560002&activo=6.do.
- (2014b): *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español*, Tesis doctoral de la Universidad de Alicante, págs. 303.
- (2015): «La desprotección "internacional" del titular del derecho a la protección de datos de carácter personal», en *BARATARIA. Revista Castellano-Manchega de Ciencias Sociales,* n. 19, págs. 37-56. ISSN: 1575-0825, e-ISSN: 2172-3184.

ORTEGA GIMÉNEZ, Alfonso, MARZO PORTERA, Ana (2013): *Empresa y transferencia internacional de datos personales*, Madrid, ICEX Instituto Español de Comercio Exterior, págs. 101.

ORTÍ VALLEJO, Antonio (1994): «El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio)», en *Derecho Privado y Constitución*, núm. 2, págs. 305-332. Disponible en Internet: http://www.cepc.gob.es/gl/publicaci%C3%B3ns/revistas/revistas-electronicas?IDR=7&IDN=376&IDA=9889.

ORTIZ LÓPEZ, Paula (2017): «Regulando la privacidad del futuro. Análisis de la Propuesta de Reglamento europeo de e-Privacy y su interconexión con el Reglamento General de Protección de Datos», en *Diario La Ley*, núm. 10, Sección Ciberderecho, 4 de octubre de 2017.

PACHECO GÓMEZ, Máximo (2000): *Los derechos humanos: documentos básicos*, tomo 3, Editorial Jurídica de Chile, págs. 1622.

PADÍN VIDAL, Alejandro (2016): «Nuevo Reglamento General de Protección de Datos de la Unión Europea», en *Lefebvre - El Derecho*, 22.04.2016. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/Reglamento-General-Proteccion-Datos-Union-Europea_11_943930002.html#a_comments.

PAGALLO, Ugo (2008): *La tutela della privacy negli Stati Uniti d'America ed in Europa. Modelli giuridici a confronto*, Milano, págs. 258.

- (2014): *Il diritto nell'età dell'informazione*, Torino, G. Giappichelli Editore, págs. 357. ISBN/EAN: 978-88-348-5835-6. Disponible en Internet: http://it.scribd.com/doc/251335183/Il-diritto-nell-eta-dell-informazione-U-Pagallo-2014#scribd.

PAJUNOJA, Lauri J. (2017): *The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU's data protection law and its compatibility with the right to privacy*, Master's thesis, University of Helsinki Faculty of law, The Erik Castrén Institute of International Law and Human Rights Public international law, págs. 96.

PALLARO, Paolo (2002): *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Milano, Giuffrè, págs. 450.

PARDOLESI, Roberto (2003) (a cura di): *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, págs. 734.

PAREJO NAVAJAS, Teresa (2010): «La Carta de los derechos fundamentales de la Unión Europea», en *Derechos y Libertades: revista de filosofía del derecho y derechos humanos*, núm. 22, época II, págs. 205-239. ISSN: 1133-0937. Disponible en Internet: https://e-archivo.uc3m.es/handle/10016/14569.

PARKIN, Joanna (2011a): «The Schengen Information System and the EU Rule of Law», en *INEX Policy Brief Centre for European Policy Studies (CEPS)*, núm. 13, págs. 9. Disponible en Internet: https://www.ceps.eu/publications/schengen-information-system-and-eu-rule-law.

- (2011b): «The Difficult Road to the Schengen Information System II: The legacy of 'laboratories' and the cost for fundamental rights and the rule of law», en *CEPS Paper in Liberty and Security in Europe*, págs. 39. Disponible en Internet: http://aei.pitt.edu/31282/1/SIS_II_paper_liberty_security_formatted1[1].pdf.

PASQUALE, Frank (2015): *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts; London, England, Harvard University Press, págs. 320.

PASTENA, Rosa (2014): «Internet e privacy: una relazione complicata (A margine della sentenza della Corte di Giustizia del 13 maggio 2014)», en *Associazione Italiana dei Costituzionalisti*, núm. 2, luglio, págs. 13. Disponible en Internet: http://www.osservatorioaic.it/internet-e-privacy-una-relazione-complicata-a-margine-della-sentenza-della-corte-di-giustizia-del-13-maggio-2014.html.

PASTOR RIDRUEJO, José Antonio (2007): «La reciente jurisprudencia del Tribunal Europeo de Derechos Humanos: temas escogidos», ponencia *Cursos de Derecho Internacional y Relaciones Internacionales de Vitoria-Gasteiz*, Madrid, pág. 239-276. Disponible en Internet: http://www.ehu.eus/cursosderechointernacionalvitoria/ponencias/pdf/2007/2007_8.pdf.

PAVÓN PÉREZ, Juan Antonio (2001): «La protección de datos personales en el Consejo de Europa: El Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los

flujos transfronterizos de datos personales», en *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, núm. 19-20, págs. 235-252. ISSN 0213-988X. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=831270.

PEERS, Steve (2012): «Analysis. The Directive on data protection and law enforcement: A Missed Opportunity?», en *Statewatch*, April, págs. 5. Disponible en Internet: http://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf.

- (2014): «The Data Retention Judgment: The CJEU Prohibits Mass Surveillance», en *EU Law Analysis*, 8 april. Disponible en Internet: http://eulawanalysis.blogspot.fi/2014/04/the-data-retention-judgment-cjeu.html.

PÉREZ ALBERDI, María Reyes (2011): «La jurisprudencia social del Tribunal Europeo de Derechos Humanos», en *LEX SOCIAL-Revista de los Derechos Sociales*, núm. 1, págs. 93-105. ISSN: 2174-6419. Disponible en Internet: https://www.upo.es/revistas/index.php/lex_social/article/viewFile/255/250.

PÉREZ DÍAZ-HEREDERO, Alberto (2016): «La evolución de la Estrategia Antiterrorista europea: Europol y sus grandes retos», en *Análisis GESI*, análisis 30. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=5684301.

PÉREZ FRANCESCH, Joan Lluís (2007): «Cooperación policial y judicial en la Convención de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, págs. 119-136. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=2492896.

- (2012): «El Tratado de Lisboa: cooperación policial y judicial entre la europeización y las reservas estatales», en SAID HUNG, Elías (Editor), *Diálogos y desafíos euro-latinoamericanos: ensayos sobre cooperación, derecho, educación y comunicación*, Barranquilla, Editorial Universidad del Norte, págs. 80-111.

PÉREZ FRANCESCH, Joan Lluís, GIL MÁRQUEZ, Tomás, GACITÚA ESPÓSITO, Alejandro (2011): «Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?», en *Institut de Ciències Polítiques i Socials (ICPS)*, WP núm. 297, Barcelona, págs. 26. Disponible en Internet: https://ddd.uab.cat/pub/worpap/2011/hdl_2072_152109/ICPS297.pdf.

PÉREZ LUÑO, Antonio Enrique (1989): «Los derechos humanos en la sociedad tecnológica», en PÉREZ LUÑO, Antonio E., GUERRERO MATEUS, M.ª Fernanda, LOSANO, Mario G., *Libertad informática y leyes de protección de datos personales*, Cuadernos y Debates, Madrid, Centro de Estudios Constitucionales, núm. 21, págs. 135-213.

PÉREZ TRIVIÑO, José Luis (1995): «Derechos humanos, relativismo y protección jurídica de la moral en el Convenio Europeo de Derechos Humanos», en *Doxa. Cuadernos de Filosofía del Derecho*, núm. 17-18, págs. 469-490. Disponible en Internet: http://www.cervantesvirtual.com/obra/derechos-humanos-relativismo-y-proteccin-jurdica-de-la-moral-en-el-convenio-europeo-de-derechos-humanos-0/.

PÉREZ, Claudi (2017): «La justicia europea falla contra el registro de pasajeros con Canadá y siembra dudas sobre el europeo», en *El País*, 26 jul. Disponible en Internet: https://elpais.com/internacional/2017/07/26/actualidad/1501059218_145408.html.

PI LLORENS, Montserrat (2001): *La Carta de los derechos fundamentales de la Unión Europea*, Edicions Universitat Barcelona, págs. 132.

PI LLORENS, Montserrat y ZAPATER DUQUE, Esther (coord.) (2014): *La dimensión exterior de las agencias del espacio de libertad, seguridad y justicia*, Madrid, Editorial Marcial Pons, págs. 218.

PIMENIDIS, Lexi, KOSTA, Eleni (2008): «The impact of the retention of traffic and location data on the internet user», en *Datenschutz und Datensicherheit - DuD*, vol. 32, issue 2, págs. 92-97.

PIÑAR MAÑAS, José Luis (2003): «El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas», en *Cuadernos de Derecho Público*, núms. 19-20, mayo-diciembre, págs. 45-90. Disponible en Internet: http://repositori.uji.es/xmlui/bitstream/handle/10234/159971/Derecho_proteccion_Pi%C3%B1ar_Ma%C3%B1as.pdf?sequence=1.

- (2009): «*Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio*», en *Fundación Alternativas*, núm. 147, págs. 72. Disponible en Internet: http://www.fundacionalternativas.org/laboratorio/documentos/documentos-de-trabajo/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio.

PIÑAR MAÑAS, José Luis (dir.), ÁLVAREZ CANO, María, RECIO GAYO, Miguel (coords.) (2017): *Reglamento general de protección de datos hacia un nuevo modelos europeo de privacidad*, Madrid, Editorial Reus, págs. 851.

PIÑAR MAÑAS, José Luis y RECIO GAYO, Miguel (2018): *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Madrid, Wolters Kluwer – La Ley, págs. 300.

PIZA, Rodolfo E., y TREJOS, Geraldo (1989): *Derecho Internacional de los derechos humanos: la Convención Americana*, San José, Costa Rica, Editorial Juricentro.

PIZZETTI, Franco (2016a): *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, G. Giappichelli Editore, págs. 328.

- (2016b): *Privacy e il diritto europeo alla protezione dei dati personali: Il Regolamento europeo 2016/679*, Torino, G. Giappichelli Editore, págs. 208.

POLLICINO, Oreste (2010): «The New Relationship between National and the European Courts after the Enlargement of Europe: Towards a Unitary Theory of Jurisprudential Supranational Law?», en *Yearbook of European Law*, vol. 29, issue 1. Disponible en Internet: https://doi.org/10.1093/yel/29.1.65.

- (2013): «Internet nella giurisprudenza delle Corti europee: prove di dialogo?», en *Forum di Quaderni Costituzionali*, núm. 1/2014, págs. 27. ISSN 2281-2113. Disponible en Internet: http://www.forumcostituzionale.it/wordpress/?p=2847.

- (2014): «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», en *federalismi.it–Focus TMT*, núm. 3, págs. 29. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?artid=28017.

POLLICINO, Oreste y BASSINI, Marco (2017): «La Corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico», en *Diritto Penale Contemporaneo*, págs. 10. Disponible en Internet: https://www.penalecontemporaneo.it/upload/POLLICINOBASSINI_2017a.pdf.

POLLICINO, Oreste, ROMEO, Graziella (2016): *The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe*, New York, Routledge, págs. 264.

POULLET, Yves (2007): «Transborder Data Flows and Extraterritoriality: The European Position», en *3Journal of International Commercial Law and Technology*, vol. 2, issue 3, págs. 141- 153. Disponible en Internet: http://www.jiclt.com/index.php/jiclt/article/view/29/28.

PRIETO GUTIERREZ, Jesús María (1997): «La Directiva 95/46/CE como criterio unificador», en *Revista del poder judicial*, núm. 48, págs. 165-234.

PUENTE ESCOBAR, Agustín (2006): «Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal», en CANALES GIL, Álvaro, BLANCO ANTÓN, María José, PIÑAR MAÑAS, José Luis, ORTUÑO SIERRA, Mercedes (coords.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Valencia, Tirant lo Blanch, págs. 37-68.

PUSATERI, Verena (2013): «La Corte EDU su contrasto al terrorismo internazionale e rispetto dei diritti fondamentali. Nota a Corte EDU, sent. 12 settembre 2012, ric. n. 10593/08, Nada c. Svizzera», en *Diritto Penale Contemporaneo*. Disponible en Internet: http://www.penalecontemporaneo.it/d/1935-la-corte-edu-su-contrasto-al-terrorismo-internazionale-e-rispetto-dei-diritti-fondamentali.

RAINER, Arnold (1998): «La Declaración Universal de Derechos Humanos y su importancia para el desarrollo de la cultura del Derecho», en BALADO RUIZ-GALLEGOS, Manuel, GARCÍA

REGUEIRO, José, DE LA FUENTE Y DE LA CALLE, Antonio María José (coords.), *La Declaración Universal de los Derechos Humanos en su 50 aniversario*, Barcelona, Bosch, págs. 59-68.

RAINEY, Bernadette, WICKS, Elizabeth and OVEY, Clare (2014): *Jacobs, White and Ovey: The European Convention on Human Rights*, 6ª ed., Oxford, Oxford University Press, págs. 728. ISBN: 9780199655083.

RALLO LOMBARTE, Artemi (2012): «Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma», en *UNED. Revista de Derecho Político*, núm. 85, septiembre-diciembre, págs. 13-56. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/10244.

- (2017): «El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en Internet», en *UNED. Teoría y Realidad Constitucional*, núm. 39, págs. 583-610. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19150.

REBOLLO DELGADO, Lucrecio (2004), *Derechos fundamentales y protección de datos*, Madrid, Dykinson, págs. 374.

- (2014): *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson, págs. 182.

REBOLLO DELGADO, Lucrecio y SERRANO PÉREZ, María Mercedes (2008): *Introducción a la protección de datos*, Madrid, Dykinson, págs. 258.

- (2010): *Introducción a la Protección de los datos*, Madrid, Dykynson, págs. 258.
- (2014): *Manual de protección de datos*, Madrid, Dikynson, págs. 354.

RECIO GAYO, Miguel (2017a): «Protección de Datos desde el Diseño: principio y obligación en el RGPD», en *Lefebvre - El Derecho*, 20.02.2017. Disponible en Internet: http://tecnologia.elderecho.com/tecnologia/privacidad/Proteccion-Datos-Diseno-obligacion-RGPD_11_1057930001.html.

- (2017b): «Normas Corporativas Vinculantes (BCRs): comentarios a los nuevos documentos de trabajo del GT29», en *Diario La Ley*, Sección Ciberderecho, núm. 1, 12 de diciembre.
- (2017c): «El consentimiento en el RGPD: comentarios al borrador de Directrices del Grupo de trabajo del artículo 29», en *Diario La Ley*, Sección Ciberderecho, núm. 1, 19 de diciembre.

RECIO, Miguel (2013): «La OCDE actualiza sus directrices sobre protección de datos», en *Lawyerpress*, 12 de septiembre.

REGI, Annalisa (2016): «La Corte Costituzionale tedesca affronta il tema dei limiti alle investigazioni compiute con strumenti di sorveglianza occulta: come contemperare il dovere dello Stato di proteggere la popolazione dalle gravi forme di criminalità con la garanzia dei diritti fondamentali della persona?», en *filodiritto.com*, 22 giugno 2016. Disponible en Internet: http://www.filodiritto.com/articoli/2016/06/la-corte-costituzionale-tedesca-affronta-il-tema-dei-limiti-alle-investigazioni-compiute-con-strumenti-di-sorveglianza.html.

REMOTTI CARBONELL, José Carlos (2007): «Las medidas contra el terrorismo en el marco del Tratado de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 181-205.

REQUEJO RODRÍGUEZ, Paloma (coord.) (2013): *Derechos y Espacio Público*, Oviedo, Ediciones de la Universidad de Oviedo, págs. 166.

RESTA, Giorgio (2016): «Il caso USA v. Apple e il dilemma dei diritti nella società della sorveglianza», en *Etica ed Economia*. Disponible en Internet: http://www.eticaeconomia.it/il-caso-usa-v-apple-e-il-dilemma-dei-diritti-nella-societa-della-sorveglianza/.

RESTA, Giorgio, ZENO-ZENCOVICH, Vincenzo (2015): *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, RomaTrE-Press, aprile, págs. 362. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/oblio.

- (2016): *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, RomaTrE-Press, págs. 373. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/PTD.

RICCIO, Giovanni M., SCORZA, Guido, BELISARIO, Ernesto (a cura di) (2018): *GDPR e Normativa Privacy Commentario*, IPSOA.

RICE, Matthew (2015): «Zakharov v Russia: A refresher on how far Europe has come», en *Privacy International*, London. Disponible en Internet: https://www.privacyinternational.org/node/688.

RIGHI, Silvia (2014): *Lotta alla criminalità e salvaguardia dei diritti e delle libertà fondamentali nell'U.E.*, Tesis Doctoral, Bologna, Alma Mater Studiorum - Università di Bologna, Dottorato di Ricerca in Diritto Europeo, Ciclo XXVI, págs. 309.

RIJKEN, Conny (2010): «Re-Balancing Security and Justice: Protection of Fundamental Rights in Police and Judicial Cooperation in Criminal Matters», en *Common Market Law Review*, vol. 47, issue 5, págs. 1455–1492.

RINOLDI, Dino Guido (2010): «Lo spazio di libertà, sicurezza e giustizia», en DRAETTA, Ugo, PARISI, Nicoletta (eds.), *Elementi di diritto dell'Unione europea. Parte speciale. Il diritto sostanziale*, Giuffrè Editore, págs. 1- 94.

- (2012): *Lo spazio di libertà, sicurezza e giustizia nel diritto dell'integrazione europea. I. Principi generali e aspetti penalistici*, Napoli, Editoriale scientifica, págs. 354. 978-88-6342-246-7.

RIPOLL CARULLA, Santiago (1990): «En torno a la calificación de la pasividad española en el cumplimiento del Convenio nº 108 de Europa como acto ilícito internacional», en *La Responsabilidad Internacional*, XIII Jornadas de la AEPDIRI, Alicante, págs. 313-330.

ROBINSON, Neil, GRAUX, Hans, BOTTERMAN, Maarten (2008): *Review of EU Data Protection Directive: Inception Report*, Santa Monica, RAND Corporation, págs. 37. Disponible en Internet: http://www.rand.org/pubs/working_papers/WR607.html.

RODRÍGUEZ-IZQUIERDO SERRANO, Miryam (2015): «El Tribunal de Justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a libertades informativas», en *Revista de Derecho Constitucional Europeo*, año 12, núm. 24, julio-diciembre. ISSN: 1697-7890. Disponible en Internet: http://www.ugr.es/~redce/REDCE24/articulos/10_RODRIGUEZ_IZQUIERDO.htm.

RODRÍGUEZ-PINA, Gloria (2016): «Por qué el PNR de la UE como medida antiterrorista puede ser ilegal», en *Huffington Post*, 14/04/2016. Disponible en Internet: http://www.huffingtonpost.es/2016/04/11/pnr-terrorismo_n_9658260.html.

ROLLA, Giancarlo (2010): «La Carta de Derechos Fundamentales de la Unión Europea y el Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales: su contribución a la formación de una jurisdicción constitucional de los derechos y las libertades», en *Revista Europea de Derechos Fundamentales*, núm. 15, págs. 15-39. Disponible en Internet: http://journals.sfu.ca/redf/index.php/redf/article/viewFile/236/229.

ROSSI, Edoardo A. (2015): «Recenti sviluppi in tema di diritto alla privacy e alla protezione dei dati personali nello spazio giuridico europeo», en *federalismi.it–Focus TMT*, núm. 2, págs. 42. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29632.

ROSSI, Lucia Serena (2012): «Does the Lisbon Treaty Provide a Clearer Separation of Competences between EU and Member States?», en BIONDI, Andrea, EECKHOUT, Piet and RIPLEY, Stefanie (eds.), *EU Law After Lisbon*, New York, págs. 472.

ROUVROY, Antoinette, POULLET, Yves (2009): «The Right to Informational Self Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy», en GUTWIRTH, Serge and others (eds.), *Reinventing Data Protection?*, Springer Netherlands, págs. 45-76.

ROVIRA, Antonio (2007): «Los defensores del pueblo y la Convención de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 207-233.

RUBECHI, Massimo (2016): «Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)», en *federalismi.it*, núm. 23, págs. 26.

RUGGERI, Stefano (2012): *Liberty and Security in Europe: a comparative analysis of pre-trial precautionary measures in criminal proceedings*, Göttingen, V&R Unipress, págs. 296.

RUILOBA ALVARIÑO, Julia (2006): «El Tribunal Europeo de Derechos Humanos: organización y funcionamiento», en *UNED. Anuario de la Escuela de Práctica Jurídica*, núm. 1, págs. 14.

ISSN: 1886-6328. Disponible en Internet: http://www2.uned.es/escuela-practica-juridica/AEPJ%201%20Julia%20Ruiloba.pdf.

RUÍZ MIGUEL, Carlos (1994): *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*, Madrid, Civitas, págs. 134. Disponible en Internet: http://www.academia.edu/25472780/El_derecho_a_la_protecci%C3%B3n_de_la_vida_privada_en_la_jurisprudencia_del_Tribunal_Europeo_de_Derechos_Humanos.

- (2003): «El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, págs. 7-43. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=635290.
- (2004): *Estudios sobre la Carta de los Derechos Fundamentales de la Unión Europea*, Universidad de Santiago de Compostela, págs. 246.

SAETTA Bruno (2016a): «Il Judicial Redress Act non tutela adeguatamente la privacy degli europei», en *BrunoSaetta.it*, 26 Febbraio. Disponible en Internet: https://brunosaetta.it/privacy/il-judicial-redress-act-non-tutela-adeguatamente-la-privacy-degli-europei.html.

- (2016b): «La sorveglianza di massa in Europa è illegale», en *Valigia blu*, 19 de abril 2016. Disponible en Internet: http://www.valigiablu.it/sorveglianza-illegale-europa/.
- (2016c): «Il Privacy Shield non è conforme alla normativa europea», en *BrunoSaetta.it*, 26 abril. Disponible en Internet: https://brunosaetta.it/privacy/privacy-shield-non-conforme-normativa-europea.html.
- (2016d): «La Corte europea dice che la sorveglianza di massa è illegittima. Di nuovo», en *Valigia Blu*, 27 diciembre. Disponible en Internet: http://www.valigiablu.it/corte-europea-sorveglianza-massa/.

SÁIZ ARNAIZ, Alejandro (2005): «El Tribunal de Justicia, los Tribunales Constitucionales y la tutela de los derechos fundamentales en la Unión Europea: entre el (potencial) conflicto y la (deseable) armonización: de los principios no escritos al catálogo constitucional, de la autoridad judicial a la normativa», en GÓMEZ FERNÁNDEZ, Itziar (coord.), CARTABIA, Marta, DE WITTE, Bruno, PÉREZ TREMPS, Pablo (dir.), *Constitución europea y constituciones nacionales*, Valencia, Tirant lo Blanch, págs. 531-588.

SALAMANCA AGUADO, Esther (2014): «El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones», en *Revista del Instituto Español de Estudios Estratégicos (IEEE)*, núm. 4, págs. 26. Disponible en: http://revista.ieee.es/index.php/ieee/article/view/137.

SALON PIEDRA, Juan Diego (2017): «La intimidad como parte de la dignidad del ser humano en el Convenio europeo de derechos humanos y la Convención americana de derechos humanos», en LÓPEZ ORTEGA, Juan José (dir.), *El Derecho a la intimidad: nuevos y viejos debates*, Madrid, Dykinson, págs. 226. ISBN: 978-84-9148-070-9. Disponible en Internet: http://e-archivo.uc3m.es/bitstream/handle/10016/24016/derecho_intimidad_2017.pdf.

SALTOR, Carlos Eduardo (2013): *La Protección de Datos Personales: Estudio Comparativo Europa-América con especial análisis de la situación Argentina*, Tesis Doctoral, Madrid, Universidad Complutense de Madrid Facultad de Derecho, págs. 504.

SALUZZO, Stefano (2016): «Tutela dei dati personali e deroghe in materia di sicurezza nazionale dopo l'entrata in vigore del "*Privacy Shield*"», en *SIDIBlog*. Disponible en Internet: http://www.sidiblog.org/2016/09/13/tutela-dei-dati-personali-e-deroghe-in-materia-di-sicurezza-nazionale-dopo-lentrata-in-vigore-del-privacy-shield/.

SÁNCHEZ BRAVO, Álvaro A. (1998): *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla, págs. 224.

SÁNCHEZ GONZÁLEZ, María Belén (2016): *Implicaciones institucionales de la ley de Protección de Datos*, Tesis doctoral, Universidad de Málaga, págs. 324. Disponible en Internet: http://riuma.uma.es/xmlui/handle/10630/11792.

SÁNCHEZ, Luisja (2016): «José Luis Piñar: "Con el nuevo Reglamento Europeo de Protección de Datos se abre una puerta a la privacidad a nivel internacional que debemos aprovechar"», en *Law&Trends*, 02/05/2016. Disponible en Internet: http://www.lawandtrends.com/noticias/tic/con-el-nuevo-reglamento-europeo-de-proteccion-de.html.

SANHERMELANDO, Juan (2016): «La Eurocámara aprueba retener los datos de los pasajeros aéreos para la lucha antiterrorista», en *El Español*, 14.04.2016. Disponible en Internet: http://www.elespanol.com/mundo/20160414/117238380_0.html.

SANTOS VARA, Juan (2003): «El desarrollo de las competencias de la Oficina Europea de Policía (EUROPOL): el control democrático y judicial», en *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, págs. 141-179. ISSN: 1138-4026. Disponible en Internet: https://dialnet.unirioja.es/servlet/articulo?codigo=635314.

SAPIENZA, Rosario (1991): «Sul margine d'apprezzamento statale nel sistema della Convenzione Europea dei Diritti dell'Uomo», en *Rivista di diritto internazionale*, vol. 74, págs. 571-614. ISSN0035-6158.

SARTOR, Giovanni, VIOLA DE AZEVEDO CUNHA, Mario (2016): «Il caso Google e i rapporti regolatori USA/EU», en RESTA, Giorgio e ZENO-ZENCOVICH, Vincenzo (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, RomaTrE-Press, págs. 99-124.

SCAFFARDI, Lucia (2017): «Data retention e diritti della persona», en *Costituzionalismo.it*, fascicolo núm. 2, Saggi e articoli - Parte II, págs. 54-87. Disponible en Internet: http://www.costituzionalismo.it/articoli/630/.

SCIROCCO, Alfonso (2008): «The Lisbon Treaty and the Protection of Personal Data in the European Union», en *European Data Protection Review*, núm. 5.

SCOTT, Mark (2015a): «Data Transfer Pact Between U.S. and Europe Is Ruled Invalid», en *The New York Times*, oct. 6. Disponible en Internet: http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=1.

- (2015b): «Europe Approves Tough New Data Protection Rules», en *The New York Times*, Dec. 15. Disponible en Internet: http://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html?_r=1.
- (2016): «U.S. and Europe in 'Safe Harbor' Data Deal, but Legal Fight May Await», en *The New York Times*, feb. 2. Disponible en Internet: http://www.nytimes.com/2016/02/03/technology/us-europe-safe-harbor-data-deal.html?_r=1.

SCHABAS, William A. (2015): *The European Convention on Human Rights*, Oxford, Oxford University Press, págs. 1440. ISBN: 9780199594061.

SCHWARTZ, Paul M. (2013): «The EU-U.S. Privacy Collision: A Turn To Institutions And Procedures», en *Harvard Law Review*, vol. 126, págs. 1966-2009. Disponible en Internet: https://harvardlawreview.org/2013/05/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/.

SERRA CRISTÓBAL, Rosario (2014): «The Impact of Counter-terrorism Security Measures on Fundamental Rights: The Need for Supranational Common Standards of Rights Protection to respond to terrorism risk», en *IXth World Congress of Constitutional Law, "Constitutional Challenges: Global and Local"*, Oslo, 16 - 20 June 2014, págs. 21. Disponible en Internet: https://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws1/w1-crist%C3%B3bal.pdf.

- (2015a): «The Impact of Counter-Terrorism Security Measures on Fundamental Rights», en *Democrazia & Sicurezza*, Università degli Studi "Roma Tre", anno V, núm. 2, págs. 17-61. Disponible en Internet: http://romatrepress.uniroma3.it/ojs/index.php/DemSic/article/view/432.
- (2015b): «La opinión pública ante la vigilancia masiva de datos. El difícil equilibrio entre acceso a la información y seguridad nacional», en *UNED. Revista de Derecho Político*, núm. 92, págs.

73-118. Disponible en Internet: http://revistas.uned.es/index.php/derechopolitico/article/view/14422.
- (2016): «Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el derecho de la Unión Europea pueden ofrecer en común», en *UNED. Teoría y Realidad Constitucional*, núm. 38, pág. 487-503. Disponible en Internet: http://e-spacio.uned.es/fez/view/bibliuned:TeoriayRealidadConstitucional-2016-38-5075.
- (2018): «El control de datos de circulación de personas en la UE como mecanismo de salvaguarda de la seguridad nacional», en *UNED. Revista de Derecho Político*, N. 102, mayo-agosto 2018, págs 305-332.

SERRANO PÉREZ, María Mercedes (2003): *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, págs. 518.

SERVIZIO STUDI DEL SENATO (2016a): *Europol ed Eurojust: l'Unione europea e la lotta al terrorismo*, dossier núm. 331, págs. 52. Disponible en Internet: https://www.senato.it/service/PDF/PDFServer/BGT/00977222.pdf.
- (2016b): «Proposta di Regolamento del Parlamento Europeo e del Consiglio che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di paese terzo o da un apolide, per l'identificazione di cittadini di paesi terzi o apolidi il cui soggiorno è irregolare e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto (rifusione)», en *Note su atti dell'Unione europea*, núm. 67, págs. 10. Disponible en Internet: https://www.senato.it/service/PDF/PDFServer/BGT/00989852.pdf.
- (2017): «Lo spazio Schengen e la sicurezza interna dell'Unione europea», en *Note su atti dell'Unione europea*, núm. 109, págs. 11. Disponible en Internet: http://www.senato.it/service/PDF/PDFServer/BGT/01022061.pdf.

SIERRA NAVA, José María (1957): *El Consejo de Europa*, Madrid, Instituto de Estudios Políticos, págs. 335.

SINGLETON, Solveig (1999): «Privacy and Human Rights: Comparing the United States to Europe», en *Cato Institute White Paper*. Disponible en Internet: https://www.cato.org/publications/white-paper/privacy-human-rights-comparing-united-states-europe.

SMITH, Graham (2014): «Dissecting DRIP - The Emergency Data Retention and Investigatory Powers Bill», en *Cyberleagle*, 12 July. Disponible en Internet: http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html.

SOMA, John T., RYNERSON, Stephen D. and BEALL-EDER, Britney D. (2004): «An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./EU E-Commerce Privacy Safe Harbor», en *Texas International Law Journal*, vol. 39, págs. 171-214. Disponible en Internet: http://www.tilj.org/content/journal/39/num2/Soma-Rynerson-Beall-Eder171.pdf.

SOMMARIO, Emanuele (2016): «Attentati di Parigi: la Francia deroga alla Convenzione Europea dei Diritti dell'Uomo», en *SIDIBlog (blog della Società italiana di diritto internazionale e di Diritto dell'Unione europea)*. Disponible en Internet: http://www.sidiblog.org/2016/01/11/attentati-di-parigi-la-francia-deroga-alla-convenzione-europea-dei-diritti-delluomo/.
- (2018): *Stati d'emergenza e trattati a tutela dei diritti umani*, G. Giappichelli, págs. 316.

SPAVENTA, Eleanor (2016): «The interpretation of Article 51 of the EU Charter of Fundamental Rights: the dilemma of stricter or broader application of the Charter to national measures», en *Study commissioned by the Policy Department for Citizen's Rights and Constitutional Affairs at the request of the PETI Committee*, PE 556.930, págs. 38. Disponible en Internet:

http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2016)556930.

STAIANO, Sandro (2017): «Diritto alla riservatezza e potere pubblico», en *federalismi.it*, núm. 17, págs. 25. Disponible en Internet: http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=34743&content=Diritto+alla+riservatezza+e+potere+pubblico&content_author=%3Cb%3ESandro+Staiano%3C/b%3E.

STANZIONE, Maria Gabriella (2016): «Il nuovo regolamento europeo sulla protezione dei dati personali: genesi e ambito di applicazione», en *Comparazione e Diritto Civile*, giugno, págs. 16. Disponible en Internet: http://www.comparazionedirittocivile.it/prova/files/Stanzione_MG_Genesi_Ambito_Applicazione_Comparazione_2016.pdf.

SURVEILLE (2014): *Surveille Paper Assessing Surveillance in the Context of Preventing a Terrorist Act*, págs. 51. Disponible en Internet: https://www.justsecurity.org/wp-content/uploads/2014/10/SURVEILLE-Paper-on-a-Terrorism-Prevention.pdf.

SY, Sarah (2017a), «Un espacio de libertad, seguridad y justicia: aspectos generales», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_5.12.1.html.

- (2017b): «La Carta de los Derechos Fundamentales de la Unión Europea», en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_1.1.6.html.

TAJADURA TEJADA, Javier (2008): «La doctrina del Tribunal Europeo de Derechos Humanos sobre la prohibición de partidos políticos», en *Boletín Mexicano de Derecho Comparado*, núm. 123, págs. 1431-1475. ISSN-e 0041-8633. Disponible en Internet: http://www.revistas.unam.mx/index.php/bmd/article/view/10779.

TEJERINA RODRÍGUEZ, Ofelia (2014): *Seguridad del Estado y privacidad*, Madrid, Editorial Reus, págs. 384.

TÉLLEZ AGUILERA, Abel (2002), *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*, Madrid, Edisofer, págs. 383.

TESAURO, Giuseppe (2012): *Diritto dell'Unione europea*, 7a ed., Padova, Cedam, págs. 960. ISBN: 978-88-13-31534-4.

TOMÁS MALLÉN, Beatriz S. (2014): «Privacidad versus seguridad en el ámbito europeo», en Antonio FAYOS GARDÓ (coord.), *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, Librería-Editorial Dykinson, págs. 215-241. ISBN: 978-84-9085-240-8.

TRAVIS, Alan (2014): «Drip Surveillance Law Faces Legal Challenge by MPs», en *The Guardian*, 22 July. Disponible en Internet: http://www.theguardian.com/world/2014/jul/22/drip-surveillance-law-legal-challenge-civil-liberties-campaigners.

- (2016): «'Snooper's charter' bill becomes law, extending UK state surveillance», en *The Guardian*, 29 November. Disponible en Internet: https://www.theguardian.com/world/2016/nov/29/snoopers-charter-bill-becomes-law-extending-uk-state-surveillance.

TRESCA, Michela (2016): «Sicurezza vs protezione dei dati: la CGUE cambia registro», en *Amministrazione in Cammino*, págs. 14. Disponible en Internet: http://www.amministrazioneincammino.luiss.it/app/uploads/2016/05/Tresca_Sicurezza-VS-protezione-dei-dati.pdf.

TRONCOSO REIGADA, Antonio (2010): *La protección de datos personales: en busca del equilibrio*, Valencia, Tirant lo Blanch, págs. 1990.

TURNER, Karen (2016): «Mass surveillance silences minority opinions, according to study», en *The Washington Post*, March 28. Disponible en Internet: https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.2f592e5d7ace.

UGARTEMENDIA ECEIZABARRENA, Juan Ignacio (2013): «La tutela judicial de los derechos fundamentales en el ámbito de aplicación nacional del derecho de la Unión Europea: recientes

acotaciones del Tribunal de Justicia y del Tribunal Constitucional Español», en *UNED. Teoría y Realidad Constitucional*, núm. 32, págs. 391-428. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/11796.

- (2017): «La eficacia entre particulares de la Carta de Derechos Fundamentales de la Unión Europea a la luz de la jurisprudencia del Tribunal de Justicia», en *UNED. Teoría y Realidad Constitucional*, núm. 39, págs. 361-386. Disponible en Internet: http://revistas.uned.es/index.php/TRC/article/view/19161.

UGARTEMENDIA ECEIZABARRENA, Juan Ignacio, ALONSO GARCÍA, Ricardo (dirs.) (2014), *La cuestión prejudicial europea*, European inklings (EUi) IV, núm. 4, págs. 201. Disponible en Internet: https://carlosesposito.files.wordpress.com/2014/05/cuestion-prejudicial-europea-dig.pdf.

VAINIO, Niklas (2016): «Fundamental rights compliance and the politics of interpretation: Explaining Member State and court reactions to Digital Rights Ireland», en BRÄUTIGAM, Tobias and MIETTINEN, Samuli, *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut, págs. 229-259.

VAINIO, Niklas, MIETTINEN, Samuli (2015): «Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States», en *International Journal of Law and Information Technology*, vol. 23, issue 3, 1. Disponible en Internet: https://doi.org/10.1093/ijlit/eav010.

VALVO, Anna Lucia (2014): «La Corte di Giustizia dichiara l'invaliditá della direttiva sulla conservazione dei dati», en *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, núm. 4. Disponible en Internet: http://www.unikore.it/index.php/indici-koreuropa/numero-4#.Vgu7N5eK-Ic.

VAN BALLEGOOIJ, Wouter and BAKOWSKI, Piotr (2018), *The Cost of Non-Europe in the fight against terrorism*, Brussels, European Added Value Unit - EPRS | European Parliamentary Research Service, PE 621.817, págs. 218. Disponible en Internet: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/621817/EPRS_STU(2018)621817_EN.pdf.

VANONI, Luca Pietro (2017): «Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems», en Forum di Quaderni Costituzionali, Rassegna núm. 6/2017. Disponible en Internet: http://www.forumcostituzionale.it/wordpress/?p=9370.

VARANI, Elena (2005): *Diritto alla privacy e trattamento dei dati sensibili in ambito sanitario. Dalla Carta dei diritti fondamentali dell'Unione Europea al decreto legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali"*, págs. 25. Disponible en Internet: https://uonted.files.wordpress.com/2008/02/varaniprivacy.pdf.

VECCHIO, Fausto (2014): «L'ingloriosa fine della direttiva Data Retention, la ritrovata vocazione costituzionale della Corte di Giustizia e il destino dell'art. 132 del Codice della Privacy», en *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, núm. 4, págs. 212-220. Disponible en Internet: http://www.unikore.it/index.php/indici-koreuropa/numero-4#.Vgu7N5eK-Ic.

VERHELLEN, Eugène (2002): *La Convención sobre los derechos del niño. Trasfondo, motivos, estrategias, temas principales*, Leuven, Garant, págs. 235.

VILASAU SOLANA, Mònica (2006): «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad», en *IDP. Revista de Internet, Derecho y Política*, núm. 3, págs. 15. ISSN: 1699-8154. Disponible en Internet: http://www.uoc.edu/idp/3/dt/esp/vilasau.html.

VIOLA DE AZEVEDO CUNHA, Mario, DONEDA, Danilo, GOMES DE ANDRADE, Norberto Nuno (2010): «The Re-Identification of Anonymous Data and the Processing of Personal Data for Further Purposes: Challenges to Privacy (La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy) (in Italian)», en

Ciberspazio e Diritto, vol. 11, núm. 4, págs. 641-655. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740383.

VIYELLA, Belén (2013): «Ley de Conservación de Datos: pros y contras de su posible modificación», en *Ecija*, 15 junio. Disponible en Internet: http://ecija.com/sala-de-prensa/ley-de-conservacion-de-datos-pros-y-contras-de-su-posible-modificacion/.

VON BERNSTORFF, Jochen (2008): «The Changing Fortunes of the Universal Declaration of Human Rights: Genesis and Symbolic Dimensions of the Turn to Rights in International Law», en *The European Journal of International Law*, vol. 19, núm. 5, págs. 903-924.

WARREN, Samuel D., BRANDEIS, Louis D. (1890): «The Right to Privacy», en *Harvard Law Review*, vol. 4, N. 5 (Dec. 15), págs. 193-220. Disponible en Internet: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

WEBER, Albrecht (2012): «The Distribution of Competences Between the Union and the Member States», en BLANKE, Hermann-Josef, MANGIAMELI, Stelio (eds.), *The European Union After Lisbon. Constitutional Basis, Economic Order and External Action*, Springer Berlin Heidelberg, págs. 584.

WIEWIÓROWSKI, Wojciech R. (2017): «Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy», en VERMEULEN, Gert, LIEVENS, Eva (Eds.), *Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data*, Antwerp-Apeldoorn-Portland, Maklu, págs. 171-192. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/17-12-18_wiewiorowski_data_protection_and_privacy_under_pressure_en.pdf

WILHELM, Ernst-Oliver (2016): «A Brief History of Safe Harbor», en *International Association of Privacy Professionals*. Disponible en Internet: https://iapp.org/resources/article/a-brief-history-of-safe-harbor/.

WOODS, Lorna (2016): «Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)», en *Eu Law Analysis*, 21 December. Disponible en Internet: http://eulawanalysis.blogspot.it/2016/12/data-retention-and-national-law-ecj.html.

WRIGHT, David (2012): «The state of the art in privacy impact assessment», en *Computer Law & Security Review*, vol. 28, págs. 54-61. Disponible en Internet: https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wright-2012e.pdf.

ZABALLOS PULIDO, Emilia (2013): *La protección de datos personales en España: evolución normativa y criterios de aplicación*, Tesis doctoral inédita de la Universidad Complutense de Madrid, Facultad de Derecho, págs. 508.

ZALNIERIUTE, Monika (2015): «An international constitutional moment for data privacy in the times of mass-surveillance», en *International Journal of Law and Information Technology*, 0, pags. 1-35. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732448.

ZAMBRANO GÓMEZ, Esperanza (2007): «La regulación de los ficheros policiales en España y su tratamiento en la Convención de Prüm. La perspectiva de las autoridades nacionales de protección de datos», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 167-180.

ZAURE, Agnes (2016): *Application of International Human Rights Online-Balancing Privacy, Freedom of Information, and National Security*, Master Thesis, University of Tartu Faculty of Law Department of Public Law, págs. 78.

ZILLER, Jacques (2007): «El Tratado de Prüm», en *Revista de Derecho Constitucional Europeo*, núm. 7, enero-junio de 2007, págs. 21-30.

TRATADOS INTERNACIONALES

DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, adoptada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948. Disponible en Internet: http://www.un.org/es/documents/udhr/law.shtml.

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Disponible en Internet: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx.

CARTA INTERNACIONAL DE DERECHOS HUMANOS.

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS (1969) (Pacto de San José).

CARTA AFRICANA SOBRE LOS DERECHOS Y EL BIENESTAR DEL NIÑO (1990).

NORMATIVA DE LA UNIÓN EUROPEA

ACUERDOS INTERNACIONALES (CONVENCIONES, TRATADOS)

CONVENIO PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL, Serie de Tratados Europeos - n. 108, Estrasburgo 28.0I.1981, ratificado por España y publicado en el *Boletín Oficial del Estado* de 15 de noviembre de 1985. Disponible en Internet: https://www.boe.es/buscar/doc.php?id=BOE-A-1985-23447.

ACERVO DE SCHENGEN - CONVENIO DE APLICACIÓN DEL ACUERDO DE SCHENGEN de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, *Diario Oficial de la Unión Europea*, L 239 de 22/09/2000, págs. 0019 – 0062. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):ES:HTML.

TRATADO DE LA UNIÓN EUROPEA, *Diario Oficial*, n. C 191 de 29/07/1992, págs. 0001 - 0110. Disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:11992M/TXT.

TRATADO DE ÁMSTERDAM POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA, LOS TRATADOS CONSTITUTIVOS DE LAS COMUNIDADES EUROPEAS Y DETERMINADOS ACTOS CONEXOS, tal como ha sido firmado el 2 de octubre de 1997 en Ámsterdam. Disponible en Internet: http://www.europarl.europa.eu/topics/treaty/pdf/amst-es.pdf.

PROTOCOLO ADICIONAL AL CONVENIO para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, Estrasburgo, 8 de noviembre de 2001. Disponible en Internet: https://rm.coe.int/16806caea0.

TRATADO POR EL QUE SE ESTABLECE UNA CONSTITUCIÓN PARA EUROPA, Roma el 29 de octubre de 2004, *Diario Oficial de la Unión Europea*, C 310 de 16 de diciembre de 2004. Disponible en Internet: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_es.pdf.

CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2007/C 303/01), *Diario Oficial de la Unión Europea*, C 303 de 14/12/2007, págs. 1-16. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:ES:PDF.

TRATADO DE LISBOA POR EL QUE SE MODIFICAN EL TRATADO DE LA UNIÓN EUROPEA Y EL TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA, *Diario - Oficial de la Unión Europea*, C 306 de 17 de diciembre de 2007. Disponible en Internet: https://www.agpd.es/portalwebAGPD/internacional/common/Trat_lisboa.pdf.

TRATADO CONSTITUTIVO DE LA COMUNIDAD EUROPEA (Vigente hasta el 1 de diciembre de 2009).

ACUERDO entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, *Diario Oficial de la Unión Europea*, L 186, 14/07/2012, págs. 4–16. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22012A0714(01).

VERSIONES CONSOLIDADAS DEL TRATADO DE LA UNIÓN EUROPEA Y DEL TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA - Protocolos - Anexos - Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa firmado el 13 de diciembre de 2007 - Tablas de correspondencias, *Diario Oficial de la Unión Europea*, núm. C 326 de 26/10/2012, págs. 0001–0390. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012M%2FTXT.

ACUERDO entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, *Diario Oficial de la Unión Europea*, L 215/5, 11.8.2012. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22012A0811(01).

ACUERDO entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales, *Diario Oficial de la Unión Europea*, L 336, 10.12.2016, págs. 3–13. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22016A1210(01).

REGLAMENTOS

REGLAMENTO (CEE) N. 2299/89 DEL CONSEJO, de 24 de julio de 1989, por el que se establece un código de conducta para los sistemas informatizados de reserva, *Diario Oficial de la Unión Europea*, L 220, 29.7.1989, págs. 1–7. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31989R2299.

REGLAMENTO (CE) N. 2725/2000 DEL CONSEJO, de 11 de diciembre de 2000, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, *Diario Oficial de la Unión Europea*, L 316 de 15.12.2000, págs. 1–10. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32000R2725.

REGLAMENTO (CE) N. 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, *Diario Oficial de la Unión Europea*, L 8 de 12.1.2001, págs. 1–22. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32001R0045.

REGLAMENTO (CE) N. 407/2002 DEL CONSEJO, de 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) n. 2725/2000 relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, *Diario Oficial de la Unión* Europea, L 062 de 05.03.2002, págs. 0001 – 0005. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32002R0407.

REGLAMENTO (CE) N. 343/2003 DEL CONSEJO, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, *Diario Oficial de la Unión Europea*, L 050 de 25.02.2003, págs. 0001 – 0010. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32003R0343.

REGLAMENTO (CE) N. 871/2004 DEL CONSEJO, de 29 de abril de 2004, relativo a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo, *Diario Oficial de la Unión Europea*, L 162 de 30/04/2004, págs. 0029 – 0031. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0871.

REGLAMENTO (CE) N. 1987/2006 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 20 de diciembre de 2006 relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), *Diario Oficial de la Unión Europea*, L 381 de 28.12.2006, págs. 4–23. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006R1987.

REGLAMENTO (CE) N. 767/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS), *Diario Oficial de la Unión Europea*, L 218 de 13.8.2008, págs. 60–81. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008R0767.

REGLAMENTO (CE) N. 810/2009 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de julio de 2009, por el que se establece un Código comunitario sobre visados (Código de visados), *Diario Oficial de la Unión Europea*, L 243 de 15.9.2009, págs. 1–58. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32009R0810.

REGLAMENTO (UE) N. 1077/2011 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, *Diario Oficial de la Unión Europea*, L 286 de 1.11.2011, págs. 1–17. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2011.286.01.0001.01.SPA&toc=OJ:L:2011:286:TOC.

REGLAMENTO (UE) N. 603/2013 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n. 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n. 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (refundición), *Diario Oficial de la Unión Europea*, L 180 de 29.6.2013, págs. 1–30. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32013R0603.

REGLAMENTO (UE) 2016/399 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen), *Diario Oficial de la Unión Europea*, L 77 de 23.3.2016, págs. 1–52. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0399.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del

EEE), *Diario Oficial de la Unión Europea*, L 119, 4.5.2016, págs. 1–88. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679.

REGLAMENTO (UE) 2016/794 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, *Diario Oficial de la Unión Europea*, L 135/53 de 24.5.2016, págs. 53–114. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0794.

REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. 45/2001 y la Decisión n. 1247/2002/CE, *Diario Oficial de la Unión Europea*, L 295/39, 21.11.2018.

REGLAMENTO (UE) 2018/1726 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de noviembre de 2018 relativo a la Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), y por el que se modifican el Reglamento (CE) n. 1987/2006 y la Decisión 2007/533/JAI del Consejo y se deroga el Reglamento (UE) n. 1077/2011.

DIRECTIVAS

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial de la Unión Europea*, L 281 de 23.11.1995, págs. 31–50. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046.

DIRECTIVA 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, *Diario Oficial de la Unión Europea*, L 024 de 30/01/1998, págs. 1–8. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31997L0066.

DIRECTIVA 2006/24/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, *Diario Oficial de la Unión Europea*, L 105, 13.4.2006, págs. 54–63. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006L0024.

DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, *Diario Oficial de la Unión Europea*, L 119, 4.5.2016, págs. 89–131. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.SPA&toc=OJ:L:2016:119:TOC.

DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, *Diario Oficial de la Unión Europea*, L 119, 4.5.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0681&from=ES.

DECISIONES

DECISIÓN DE LA COMISIÓN, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C(2000) 2441] (Texto pertinente a efectos del EEE.), 2000/520/CE, *Diario Oficial de la Unión Europea*, L 215, 25.8.2000, págs. 7–47. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32000D0520.

DECISIÓN DEL CONSEJO, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (2002/187/JAI), *Diario Oficial de la Unión Europea*, L 063 de 06/03/2002, págs. 0001 – 0013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32002D0187.

DECISIÓN MARCO 2002/584/JAI DEL CONSEJO, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros, *Diario Oficial de la Unión Europea*, L 190 de 18.07.2002, págs. 0001 – 0020.

DECISIÓN DE LA COMISIÓN de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (*Bureau of Customs and Border Protection*) *[notificada con el número C(2004) 1914]*, (Texto pertinente a efectos del EEE), (2004/535/CE), *Diario Oficial de la Unión Europea*, L 235, 6.7.2004. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/Decisi-oo-n-sobre-datos-pasajeros-USA.pdf.

DECISIÓN DEL CONSEJO de 17 de mayo de 2004 relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (2004/496/CE), *Diario Oficial de la Unión Europea*, L 183/83, 20.5.2004. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOL_2004_183_R_0083_01.

DECISIÓN DEL CONSEJO, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE), *Diario Oficial de la Unión Europea*, L 213 de 15.6.2004, págs. 5–7. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32004D0512.

DECISIÓN 2005/211/JAI DEL CONSEJO de 24 de febrero de 2005 relativa a la introducción de nuevas funciones para el Sistema de Información de Schengen, inclusive en materia de lucha contra el terrorismo, *Diario Oficial de la Unión Europea*, L 68 de 15.3.2005. Disponible en Internet: https://www.unodc.org/tldb/pdf/2005-211-JAI_ES.pdf.

DECISIÓN 2006/729/PESC/JAI DEL CONSEJO, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, *Diario Oficial de la Unión Europea*, L 298, 27.10.2006, págs. 27–31. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOL_2006_298_R_0027_01.

DECISIÓN MARCO 2006/960/JAI DEL CONSEJO, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, *Diario Oficial de la Unión Europea*, L 386 de 29.12.2006, págs. 89–100. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32006F0960.

DECISIÓN 2007/533/JAI DEL CONSEJO, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), *Diario Oficial de la Unión Europea*, L 205 de 7.8.2007, págs. 63–84. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32007D0533.

DECISIÓN 2007/551/PESC/JAI DEL CONSEJO, de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo *PNR* 2007). Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (*PNR*) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo *PNR* 2007), *Diario Oficial de la Unión Europea*, L 204, 4.8.2007, págs. 16–25. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2007.204.01.0016.01.SPA.

DECISIÓN 2008/615/JAI DEL CONSEJO, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, L 210 de 6.8.2008, págs. 1–11. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008D0615.

DECISIÓN 2008/616/JAI DEL CONSEJO, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, L 210 de 6.8.2008, págs. 12–72. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008D0616.

DECISIÓN 2008/633/JAI DEL CONSEJO, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, *Diario Oficial de la Unión Europea*, L 218 de 13.8.2008, págs. 129–136. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32008D0633.

DECISIÓN MARCO 2008/977/JAI DEL CONSEJO, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, *Diario Oficial de la Unión Europea*, L 350 de 30.12.2008, págs. 60–71. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32008F0977.

DECISIÓN DEL CONSEJO de 26 de abril de 2012 relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (2012/472/UE), *Diario Oficial de la Unión Europea*, L 215/4, 11.8.2012. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:JOL_2012_215_R_0004_01&from=IT.

DECISIÓN DEL CONSEJO, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) (2009/371/JAI), *Diario Oficial de la Unión Europea*, L 121 de 15.5.2009, págs. 37–66. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32009D0371.

DECISIÓN DEL CONSEJO DE 7 DE MARZO DE 2013, por la que se fija la fecha de aplicación de la Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (2013/157/UE), *Diario Oficial de la Unión Europea*, L 87 de 27.03.2013, págs. 8-9. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013D0157.

DECISIÓN DEL CONSEJO de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (2014/415/UE), *Diario Oficial de la Unión Europea*, L

192 de 1.7.2014, págs. 53–58. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32014D0415.

DECISIÓN DE EJECUCIÓN (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU., *Diario Oficial de la Unión Europea*, L 207, 1.8.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016D1250.

JURISPRUDENCIA DE INTERÉS

JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS (TEDH)

Abdullah Öcalan contra Turquía, números 24069/03, 197/04, 6201/06 y 10464/07, sentencia de 18 de marzo de 2014. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-142086#{"itemid":["001-142086"]}.

Allan contra el Reino Unido, núm. 48539/99, sentencia de 5 de noviembre de 2002. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-60713#{"itemid":["001-60713"]}.

Amann contra Suiza [GS], núm. 27798/95, sentencia de 16 de febrero de 2000. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-58497#{%22itemid%22:[%22001-58497%22]}.

B.B. contra Francia, núm. 5335/06, sentencia de 17 de diciembre de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-96361#{"itemid":["001-96361"]}.

Brunet contra Francia, núm. 21010/10, sentencia de 18 de septiembre de 2014. Disponible en Internet: https://hudoc.echr.coe.int/eng#{"itemid":["001-146389"]}.

Copland contra el Reino Unido, núm. 62617/00, sentencia de 3 de julio de 2007. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-79996#{%22itemid%22:[%22001-79996%22]}.

Dalea contra Francia, núm. 964/07, sentencia de 2 de febrero de 2010. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["863599"],"itemid":["001-97520"]}.

Gardel contra Francia, núm. 16428/05, sentencia de 17 de marzo de 2010. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-96457#{"itemid":["001-96457"]}.

Gillan y Quinton contra Reino Unido, núm. 4158/05, sentencia de 12 enero 2010. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-139040#{"itemid":["001-139040"]}.

Haralambie contra Rumania, núm. 21737/03, sentencia de 27 de octubre de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["856690"],"itemid":["001-95302"]}.

Irlanda contra Reino Unido, núm. 5310/71, sentencia de 18 de enero de 1978. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57506#{"itemid":["001-57506"]}.

K.U. contra Finlandia, núm. 2872/02, sentencia de 2 de marzo de 2009. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-89964#{%22itemid%22:[%22001-89964%22]}.

Klass y otros contra Alemania, núm. 5029/71, sentencia de 6 de septiembre de 1978. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57510.

Kopp contra Suiza, núm. 23224/1994, sentencia de 25 de marzo de 1998. Disponible en Internet: http://lawcenter.es/w/file/download/66097.

Kruslin contra Francia, núm. 11801/85, sentencia de 23 de abril de 1990. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"fulltext":["Kruslin"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57626"]}.

Leander contra Suecia, núm. 9248/81, sentencia de 26 de marzo de 1987. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57519#{%22itemid%22:[%22001-57519%22]}.

M.S. contra Suecia, núm. 20837/92, sentencia de 27 de agosto de 1997. Disponible en Internet: http://www.bailii.org/eu/cases/ECHR/1997/49.html.

Malone contra el Reino Unido, núm. 8691/79, sentencia de 02 de agosto de 1984. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57533#{%22itemid%22:[%22001-57533%22]}.
Marckx contra Belgium, núm. 6833/74, sentencia de 13 junio de 1979. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57534#{%22itemid%22:[%22001-57534%22]}.
Nada contra Suiza, núm. 10593/08, sentencia de 12 de septiembre de 2012. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-113121#{"itemid":["001-113121"]}.
Niemietz contra Alemania, núm. 13710/88, sentencia de 16 de diciembre de 1992. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57887#{"itemid":["001-57887"]}.
Roman Zakharov contra Rusia, núm. 47143/06, sentencia de 4 de diciembre de 2015. Disponible en Internet: http://hudoc.echr.coe.int/fre?i=001-159324#{"itemid":["001-159324"]}.
Rotaru contra Romania [GS], núm. 28341/95, sentencia de 04 de mayo de 2000. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"appno":["28341/95"],"itemid":["001-58586"]}
S. and Marper contra Reino Unido, núm. 30562/04 y núm. 30566/04, sentencia de 4 de diciembre de 2008. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-90051#{%22itemid%22:[%22001-90051%22]}.
Shimovolos contra Rusia, núm. 30194/09, sentencia de 21 de junio de 2011. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"dmdocnumber":["886752"],"itemid":["001-105217"]}.
Szabó and Vissy contra Hungría, núm. 37138/14, sentencia de 12 de enero de 2016. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-160020#{"itemid":["001-160020"]}.
Taylor-Sabori contra el Reino Unido, núm. 47114/99, de 22 de octubre de 2002.
Valenzuela Contreras contra España, núm. 58/1997/842/1048, sentencia de 30 de junio de 1998. Disponible en Internet: http://hudoc.echr.coe.int/eng#{"fulltext":["Valenzuela"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-58208"]}.
Vetter contra Francia, núm. 59842/00, sentencia de 31 de mayo de 2005. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-69188#{"itemid":["001-69188"]}.
X e Y contra Holanda, núm. 8978/80, sentencia de 26 de marzo de 1985. Disponible en Internet: https://www.coe.int/t/dg2/equality/domesticviolencecampaign/resources/X%20AND%20Y%20v%20THE%20NETHERLANDS_en.asp.
X e Y contra los Países Bajos, núm. 8978/80, sentencia de 26 marzo de 1985. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-57603#{%22itemid%22:[%22001-57603%22]}.
Z. contra Finlandia, núm. 22009/93, sentencia de 25 de febrero de 1997. Disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-58033#{%22itemid%22:[%22001-58033%22]}.

JURISPRUDENCIA, DICTÁMENES, RECURSOS Y OTROS DOCUMENTOS DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (TJUE)

Åklagaren y Hans Åkerberg Fransson, (Gran Sala), asunto C-617/10, sentencia de 26 de febrero de 2013. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=134202&doclang=ES.
Association Belge des Consommateurs Test-Achats ASBL y otros contra Conseil des ministres, asunto C-236/09, sentencia de 1 de marzo de 2011. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=80019&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=35196.
Bodil Lindqvist, asunto C-101/01, sentencia de 6 de noviembre de 2003. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9409.
Comisión de las Comunidades Europeas contra Reino de España, (Gran Sala), asunto C-503/03, sentencia de 31 de enero de 2006. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=55480&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=366833.

Comisión de las Comunidades Europeas contra República Helénica, asunto C-475/01, sentencia de 5 de octubre de 2004.

Comisión Europea contra Hungría, (Gran Sala), asunto C-288/12, sentencia de 8 de abril de 2014.

Comisión Europea contra República de Austria, (Gran Sala), asunto C-614/10, sentencia de 16 de octubre de 2012. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/index-ides-idphp.php.

Comisión Europea contra República Federal de Alemania, (Gran Sala), asunto C-518/07, sentencia de 9 de marzo de 2010. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/index-ides-idphp.php.

Comisión Europea contra The Bavarian Lager Co. Ltd, Supervisor Europeo de Protección de Datos (SEPD), (Gran Sala), asunto C-28/08 P, sentencia de 29 de junio de 2010. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=81476&doclang=ES&mode=&part=1

Costa contra Enel, asunto 6/64, sentencia de 15 de julio de 1964. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61964CJ0006&from=IT.

Digital Rights Ireland Ltd y Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General y Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros, (Gran Sala), asuntos acumulados C-293/12 y C-594/12, sentencia de 8 de abril de 2014. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1187321.

Erich Stauder contra Stadt Ulm – Sozialamt, asunto 29/69, sentencia de 12 de noviembre de 1969. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61969CJ0029&from=EN.

Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos, Mario Costeja González, (Gran Sala), asunto C-131/12, sentencia de 13 mayo de 2014. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES#Footref*.

Göta hovrätt (Suecia) contra Bodil Lindqvist, asunto C-101/01, sentencia de 6 de noviembre de 2003. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/index-ides-idphp.php.

Institut professionnel des agents immobiliers (IPI) contra Geoffrey Englebert, Immo 9 SPRL, Grégory Francotte, (Sala Tercera), asunto C-473/12, sentencia de 7 de noviembre de 2013. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/index-ides-idphp.php.

Internationale Handelsgesellschaft mbH contra Einfuhr- und Vorratsstelle für Getreide und Futtermittel, asunto 11/70, sentencia de 17 de diciembre de 1970. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61970CJ0011&from=ES.

Irlanda contra Parlamento Europeo y Consejo de la Unión Europea, (Gran Sala), asunto C-301/06, sentencia de 10 de febrero de 2009. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=72843&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=194584.

J. Nold, Kohlen-und Baustoffgroßhandlung contra Commission des Communautés européennes, asunto 4-73, sentencia de 14 de mayo de 1974. Disponible en Internet: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?isOldUri=true&uri=CELEX:61973CJ0004.

Land Baden-Württemberg y Panagiotis Tsakouridis, (Gran Sala), asunto C-145/09, sentencia de 23 de noviembre de 2010. Disponible en Internet:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=79729&pageindex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=205778.

Maximillian Schrems contra Data Protection Commissioner, (Gran Sala), asunto C-362/14, sentencia de 6 de octubre de 2015. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf;?docid=169195&doclang=ES.

National Panasonic (UK) Limited contra Comisión de las Comunidades Europeas, asunto 136/79, sentencia de 26 de junio de 1980. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61979CJ0136&from=IT.

NV (Sociedad Anónima) Algemene Transport- en Expeditie Onderneming van Gend & Loos contra Nederlandse administratie der belastingen (Administración Tributaria neerlandesa), asunto 26/62, sentencia de 5 de febrero de 1963. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61962CJ0026&from=IT.

Osman Ocalan, Serif Vanly y Consejo de la Unión Europea, (Sala Primera), asunto C-229/05 P, sentencia de 18 de enero de 2007. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=65123&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1875075.

Österreichischer Rundfunk, asuntos acumulados C-465/00, C-138/01 y C-139/01, sentencia de 20 de mayo de 2003. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=48330&doclang=ES.

Parlamento Europeo contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas, (Gran Sala), asuntos acumulados C-317/04 y C-318/04, sentencia de 30 de mayo de 2006. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=635858.

Reino Unido de Gran Bretaña y de Irlanda del Norte contra Consejo de la Unión Europea, (Gran Sala), asunto C-482/08, sentencia de 26 de octubre de 2010. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=78737&doclang=ES.

Rolland Rutili y Ministerio del Interior, asunto 36/75, sentencia de 28 de octubre de 1975. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61975CJ0036&from=FR.

Stefano Melloni y Ministerio Fiscal, (Gran Sala), asunto C-399/11, sentencia de 26 de febrero de 2013. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=134203&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1846016.

Stichting Al-Aqsa y Consejo de la Unión Europea, (Sala Tercera), asuntos acumulados C-539/10 P y C-550/10 P, sentencia de 15 de noviembre de 2012. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=129846&pageindex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=205778.

Tele2 Sverige AB y Post- och telestyrelsen, y Secretary of State for the Home Department y Tom Watson, Peter Brice, Geoffrey Lewis, (Gran Sala), asuntos acumulados C-203/15 y C-698/15, sentencia de 21 de diciembre de 2016. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1168303.

Volker und Markus Schecke GbR (C-92/09), *Hartmut Eifert* (C-93/09) *y Land Hessen*, (Gran Sala), asuntos acumulados C-92/09 y C-93/09, sentencia de 9 de noviembre de 2010. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1680152.

Yassin Abdullah Kadi y Al Barakaat International Foundation contra Consejo de la Unión Europea y Comisión de las Comunidades Europeas, (Gran Sala), asuntos acumulados C-402/05 P y C-415/05 P, sentencia de 3 de septiembre de 2008. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62005CJ0402.

Yvonne van Duyn y Home Office, asunto 41/74, sentencia de 4 de diciembre de 1974. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:61974CJ0041&from=IT.

CONCLUSIONES DEL ABOGADO GENERAL Sr. Yves Bot, presentadas el 23 de septiembre de 2015, asunto C-362/14. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=326249.

CONCLUSIONES DEL ABOGADO GENERAL Sr. Henrik Saugmandsgaard Øe, presentadas el 19 de julio de 2016, Asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen* (C-203/15) y *Secretary of State for the Home Department contra Tom Watson, Peter Brice, Geoffrey Lewis* (C-698/15). Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=ES.

CONCLUSIONES DEL ABOGADO GENERAL Sr. Paolo Mengozzi, presentadas el 8 de septiembre de 2016, Dictamen 1/15, Solicitud de dictamen presentada por el Parlamento Europeo. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=216001.

COURT OF JUSTICE OF THE EUROPEAN UNION - Press Release (2017): The Court declares that the agreement envisaged between the European Union and Canada on the transfer of Passenger Name Record data may not be concluded in its current form, núm. 84/17, Luxembourg, 26 July 2017. Disponible en Internet: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf.

DICTAMEN DEL TRIBUNAL DE JUSTICIA (Pleno) de 18 de diciembre de 2014. Dictamen emitido en virtud del artículo 218 TFUE, apartado 11. Dictamen 2/13. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/SUM/?uri=CELEX:62013CV0002.

RECURSO INTERPUESTO el 16 de septiembre de 2016 - Digital Rights Ireland/Comisión, asunto T-670/16, *Diario Oficial de la Unión Europea*, C 410, 7.11.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62016TN0670.

RECURSO INTERPUESTO el 25 de octubre de 2016 - La Quadrature du Net y otros/Comisión, asunto T-738/16, *Diario Oficial de la Unión Europea*, C 6, 9.1.2017. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:62016TN0738.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA - Comunicado de prensa núm. 180/14: El Tribunal de Justicia se pronuncia sobre el Proyecto de acuerdo de adhesión de la Unión Europea al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales e identifica problemas de compatibilidad con el Derecho de la Unión, dictamen 2/13, Luxemburgo, 18 de diciembre de 2014. Disponible en Internet: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-12/cp140180es.pdf.

DOCUMENTOS DEL PARLAMENTO EUROPEO

DECLARACIÓN COMÚN DEL PARLAMENTO EUROPEO, DEL CONSEJO Y DE LA COMISIÓN, *Diario Oficial*, n. C 103 de 27/04/1977, págs. 0001 – 0002. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31977Y0427(01).

DOCUMENTO DE TRABAJO sobre una Decisión del Consejo relativa a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, 10.4.2007, págs. 6. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824es.pdf.

EUROPEAN PARLIAMENT - Committee on Civil Liberties, Justice and Home Affairs (2013a), AMENDMENTS (10) 2951 – 3133, Draft report Jan Philipp Albrecht (PE501.927v04-00), 2012/0011(COD), 8.3.2013. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/929/929832/929832en.pdf.

EUROPEAN PARLIAMENT - Committee on Civil Liberties, Justice and Home Affairs (2013b): LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens - Final programme, Brussels, 14 October 2013. Disponible en Internet: http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20131014_1500.htm.

EUROPEAN PARLIAMENT - Press Releases (2013): Civil Liberties MEPs pave the way for stronger data protection in the EU, 21-10-2013. Disponible en Internet: http://www.europarl.europa.eu/news/en/news-room/20131021IPR22706/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU.

EUROPEAN PARLIAMENT - Press Releases (2016): EU PNR: useful against terrorism, but privacy and proportionality worries remain, 13-04-2016. Disponible en Internet: http://www.europarl.europa.eu/news/en/press-room/20160408IPR22127/eu-pnr-useful-against-terrorism-but-privacy-and-proportionality-worries-remain.

EUROPEAN PARLIAMENT (2016): EU Passenger Name Record (PNR) directive: an overview, 01-06-2016, págs. 15. Disponible en Internet: http://www.europarl.europa.eu/pdfs/news/expert/background/20150123BKG12902/20150123BKG12902_en.pdf.

EXPLICACIONES SOBRE LA CARTA DE LOS DERECHOS FUNDAMENTALES (2007/C 303/02), *Diario Oficial de la Unión Europea*, C 303 de 14.12.2007, págs. 17–35. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32007X1214(01).

INFORME sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior, (2013/2188(INI)), 21 de febrero de 2014. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES.

INFORME SOBRE LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (versión refundida) (COM(2016)0272 – C8-0179/2016 – 2016/0132(COD)), 9 de junio de 2017.

INFORME SOBRE LA PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 22 de noviembre de 2013. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0402+0+DOC+XML+V0//ES#title2.

PARLAMENTO EUROPEO - Notas de prensa (2013): Civil Liberties Committee rejects EU Passenger Name Record proposal, 24-04-2013. Disponible en Internet: http://www.europarl.europa.eu/news/es/press-room/20130422IPR07523/civil-liberties-committee-rejects-eu-passenger-name-record-proposal.

PARLAMENTO EUROPEO - Notas de prensa (2014b): La Eurocámara refuerza la protección de datos de los europeos en la era digital, Sesión plenaria, 12-03-2014. Disponible en Internet:

http://www.europarl.europa.eu/news/es/news-room/content/20140307IPR38204/html/La-Euroc%C3%A1mara-refuerza-la-protecci%C3%B3n-de-datos-de-los-europeos-en-la-era-digital.

PARLAMENTO EUROPEO - Notas de prensa (2016a): El Parlamento aprueba la directiva sobre registro de datos de pasajeros (PNR), 14-04-2016. Disponible en Internet: http://www.europarl.europa.eu/news/es/news-room/20160407IPR21775/el-parlamento-aprueba-la-directiva-sobre-registro-de-datos-de-pasajeros-(pnr).

PARLAMENTO EUROPEO - Notas de prensa (2016b): Reforma de la protección de datos - Nuevas reglas adaptadas a la era digital, 14-04-2016, http://www.europarl.europa.eu/news/es/news-room/20160407IPR21776/Reforma-de-la-protecci%C3%B3n-de-datos-%E2%80%93-Nuevas-reglas-adaptadas-a-la-era-digital.

PARLAMENTO EUROPEO - Notas de prensa (2014a): EE.UU. debe poner fin al espionaje masivo o afrontar las consecuencias, advierte el PE, 12-03-2014. Disponible en Internet: http://www.europarl.europa.eu/news/es/news-room/20140307IPR38203/ee.uu.-debe-poner-fin-al-espionaje-masivo-o-afrontar-las-consecuencias.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011, COM(2017) 352 final - 2017/0145 (COD), Brussels, 29.6.2017. Disponible en Internet: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170629_proposal_for_a_regulation_on_eulisa_en.pdf.

PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1987/2006, COM(2016) 882 final - 2016/0408(COD), Bruxelles, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52016PC0882R(01).

PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica il regolamento (UE) n. 515/2014 e abroga il regolamento (CE) n. 1986/2006, la decisione 2007/533/GAI del Consiglio e la decisione 2010/261/UE della Commissione, COM(2016) 883 final - 2016/0409 (COD), Bruxelles, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52016PC0883&from=EN.

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, COM/2011/0032 final - COD 2011/0023, Bruselas, 2.2.2011. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52011PC0032.

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, Bruselas, 25.1.2012, COM/2012/010 final, 2012/0010 (COD). Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0010.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la Agencia de la Unión Europea para la cooperación y la formación en funciones coercitivas (Europol) y por el que se derogan las Decisiones 2009/371/JAI y 2005/681/JAI, COM(2013) 173 final, Bruselas, 27.3.2013. Disponible en Internet:

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0173_/com_com(2013)0173_es.pdf.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n. 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida] y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (refundición), COM(2016) 272 final - 2016/0132 (COD), Bruselas, 4.5.2016. Disponible en Internet: https://ec.europa.eu/transparency/regdoc/rep/1/2016/ES/1-2016-272-ES-F1-1.PDF.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), Bruselas, 25.1.2012, COM/2012/011 final, 2012/0011 (COD). Disponible en Internet: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular, COM(2016) 881 final - 2016/0407(COD), Bruselas, 21.12.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016PC0881.

PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM(2017) 10 final, 2017/0003(COD), Bruselas, 10.1.2017. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0010.

PROPUESTA DE RESOLUCIÓN tras una declaración de la Comisión presentada de conformidad con el artículo 123, apartado 2, del Reglamento interno sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU (2018/2645(RSP)), B8-0305/2018, 26.6.2018.

RESOLUCIÓN DEL PARLAMENTO EUROPEO sobre los flujos transatlánticos de datos (2016/2727(RSP)), 24.5.2016. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P8-RC-2016-0623+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI)). Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 22 de mayo de 2012, sobre la Estrategia de Seguridad Interior de la Unión Europea (2010/2308(INI)), Martes 22 de mayo de 2012 - Estrasburgo, P7_TA(2012)0207. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0207+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2009, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada “Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos − Programa de Estocolmo”, 25 de noviembre de 2009 – Estrasburgo, P7_TA(2009)0090. Disponible en Internet:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009-0090+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2014, sobre la solicitud al Tribunal de Justicia de un dictamen sobre la compatibilidad con los Tratados del Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros, (2014/2966(RSP)). Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0058+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2015, sobre la prevención de la radicalización y el reclutamiento de ciudadanos europeos por organizaciones terroristas (2015/2063(INI)), Miércoles 25 de noviembre de 2015 – Estrasburgo, P8_TA(2015)0410. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0410+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 25 de noviembre de 2015, sobre la prevención de la radicalización y el reclutamiento de ciudadanos europeos por organizaciones terroristas (2015/2063(INI)), Miércoles 25 de noviembre de 2015 - Estrasburgo, P8_TA(2015)0410. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0410+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos (2016/2727(RSP)), Bruselas, Jueves 26 de mayo de 2016. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 29 de octubre de 2015, sobre el seguimiento de la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la vigilancia electrónica masiva de los ciudadanos de la UE (2015/2635(RSP)), Jueves 29 de octubre de 2015 - Estrasburgo, P8_TA(2015)0388. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en la privacidad de los ciudadanos de la UE (2013/2682(RSP)), Jueves 4 de julio de 2013 - Estrasburgo. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 5 de mayo de 2010, sobre el inicio de las negociaciones para los acuerdos relativos al registro de nombres de los pasajeros (PNR) con los Estados Unidos, Australia y Canadá, *Diario Oficial de la Unión Europea*, C 81E, 15.3.2011, págs. 70–74. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010IP0144.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 6 de abril de 2017, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. (2016/3018(RSP)). Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0131+0+DOC+XML+V0//ES.

RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)), 6 de julio de 2011 – Estrasburgo, P7_TA(2011)0323. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES.

RESOLUCIÓN LEGISLATIVA DEL PARLAMENTO EUROPEO, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura), Miércoles 12 de marzo de 2014 - Estrasburgo. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES.

DOCUMENTOS CONSEJO DE LA UNIÓN EUROPEA

ACTO DEL CONSEJO, de 26 de julio de 1995, relativo al establecimiento del Convenio, basado en el artículo K.3 del Tratado de la Unión Europea, por el que se crea una Oficina Europea de Policía (Convenio Europol), *Diario Oficial*, C 316 de 27.11.1995, pág. 0001. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995F1127(01).

CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015b): Protección de datos: el Consejo acuerda una orientación general, 450/15, 15.6.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/06/15-jha-data-protection/.

CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015c), Protección de datos con fines de cooperación policial y judicial en materia penal: el Consejo, preparado para las conversaciones con el Parlamento Europeo, 712/15, 09.10.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/10/09-data-protection/.

CONCLUSIONES de la Presidencia del Consejo Europeo de Sevilla 21 y 22 de junio de 2002, 13463/02, Bruselas, 24 de octubre de 2002 (29.10), págs. 42. Disponible en Internet: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/es/ec/72639.pdf.

CONSEJO DE LA UNIÓN EUROPEA (2009): 2009 Catálogo de Schengen. Recomendaciones y prácticas más idóneas SIS, 16613/3/08, REV 3, Bruselas, 8 de mayo de 2009 (29.05), págs. 31. Disponible en Internet: http://www.intermigra.info/archivos/impresos/CatScheng.pdf.

CONSEJO DE LA UNIÓN EUROPEA (2014b): Consejo de Justicia y Asuntos de Interior, 09-10.10.2014, Sesión n. 3336, Luxemburgo, 9.10.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/10/09-10/.

CONSEJO DE LA UNIÓN EUROPEA (2014c): Consejo de Justicia y Asuntos de Interior, 4-5.12.2014, Sesión n. 3354, Bruselas, 4-5.12.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/12/04-05/.

INFORME sobre la aplicación de la declaración de los miembros del Consejo Europeo de 12 de febrero de 2015, de las Conclusiones del Consejo JAI de 20 de noviembre de 2015 y de las Conclusiones del Consejo Europeo de 18 de diciembre de 2015, 6785/16, Bruselas, 4 de marzo de 2016, págs. 46. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6785-2016-INIT/es/pdf.

POSICIÓN DEL CONSEJO en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) - Adoptada por el Consejo el 8 de abril de 2016, 5419/1/16 REV 1, 2012/0011 (COD), Bruselas, 8 de abril de 2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_5419_2016_REV_1&qid=1463305162724&from=ES.

COUNCIL OF THE EUROPEAN UNION - Press Release (2014): 3298th Council meeting, Justice and Home Affairs, Brussels, 3 and 4 March 2014, 7095/14. Disponible en Internet: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/jha/141295.pdf.

PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 11624/1/13, REV 1, Brussels, 2 October 2013, págs. 88. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-11624-2013-REV-1/en/pdf.

PROPOSAL FOR A DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Chapters I-IV, 14901/2/13, REV 2, Brussels, 30 October 2013, págs. 121. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-14901-2013-REV-2/en/pdf.

COUNCIL OF THE EUROPEAN UNION (2014b): Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council's preparatory bodies, 13390/14, Brussels, 29 September 2014. Disponible en Internet: http://statewatch.org/news/2014/oct/eu-council-fundamental-rights-guidelines-13390-14.pdf.

EL PROGRAMA DE LA HAYA: CONSOLIDACIÓN DE LA LIBERTAD, LA SEGURIDAD Y LA JUSTICIA EN LA UNIÓN EUROPEA, *Diario Oficial de la Unión Europea*, C 53 de 3.3.2005, págs. 1–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52005XG0303(01).

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - The one-stop-shop mechanism, 2012/0011 (COD), 6833/15, Brussels, 9 March 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf#http://data.consilium.europa.eu/doc/document/ST-6833-2015-INIT/en/pdf%20.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Chapter II, 2012/0011 (COD), 6834/15, Brussels, 9 March 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-6834-2015-INIT/en/pdf.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach, 2012/0011 (COD), 9565/15, Brussels, 11 June 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation for trilogue, 2012/0011 (COD), 9985/1/15, REV 1, Brussels, 11 June 2015. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-9985-2015-REV-1/en/pdf.

PROPUESTA DE DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a la datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de protección de las personas físicas en lo que respecta al tratamiento de dichos datos − Orientación general, 12555/15, Bruselas, 2 de octubre de 2015, págs. 76. Disponible en Internet: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/es/pdf.

RESOLUCIÓN DEL CONSEJO DE 17 DE ENERO DE 1995 sobre la interceptación legal de las telecomunicaciones, *Diario Oficial n. C 329 de 04/11/1996 p. 0001 – 0006*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31996G1104.

SESIÓN EXTRAORDINARIA DEL CONSEJO - JUSTICIA, ASUNTOS DE INTERIOR Y PROTECCIÓN CIVIL, C/01/327, Bruselas, 20 de septiembre de 2001. Disponible en Internet: http://europa.eu/rapid/press-release_PRES-01-327_es.htm.

CONSEJO DE LA UNIÓN EUROPEA (2014a): Consejo de Justicia y Asuntos de Interior, 05-6.6.2014, Sesión n. 3319, Luxemburgo, 5.6.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/jha/2014/06/05-06/.

COUNCIL OF THE EUROPEAN UNION (2014a): Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12, 9009/14, Brussels, 5 May 2014, págs. 8. Disponible en Internet: http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf.

CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015a): Protección de datos: El Consejo llega a un acuerdo sobre los principios generales y el mecanismo de ventanilla única, 114/15, 13.3.2015. Disponible en Internet: http://www2.consilium.europa.eu/es/press/press-releases/2015/03/13/data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/.

CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2015d): Conclusiones del Consejo de la UE y de los Estados miembros reunidos en el Consejo en materia de lucha antiterrorista, 20.11.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/11/20-jha-conclusions-counter-terrorism/.

CONSEJO DE LA UNIÓN EUROPEA (2016), Hoja de ruta para mejorar el intercambio y la gestión de la información, con inclusión de soluciones de interoperabilidad en el ámbito de la Justicia y los Asuntos de Interior, 9368/1/16, Bruselas, 6 de junio de 2016, págs. 56.

DOCUMENTOS DE LA COMISIÓN EUROPEA

COMISIÓN EUROPEA - Comunicado de prensa (2007): Carta de los Derechos Fundamentales: los Presidentes de la Comisión Europea, del Parlamento y del Consejo firman y proclaman solemnemente la Carta en Estrasburgo, IP/07/1916, Bruselas, 12 de diciembre de 2007. Disponible en Internet: http://europa.eu/rapid/press-release_IP-07-1916_es.htm.

COMISIÓN EUROPEA - Comunicado de Prensa (2012): La Comisión propone una reforma general de las normas de protección de datos para aumentar el control de los usuarios sobre sus propios datos y reducir los costes para las empresas, Bruselas, 25 de enero de 2012. Disponible en Internet: http://europa.eu/rapid/press-release_IP-12-46_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2014a): Día de la Protección de Datos 2014: la vicepresidenta Reding aboga por un nuevo pacto europeo en materia de protección de datos, Bruselas, 28 de enero de 2014. Disponible en Internet: http://europa.eu/rapid/press-release_IP-14-70_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2014b): Una nueva era para las políticas de justicia e interior de la UE, Bruselas, 01 diciembre 2014. Disponible en Internet: http://europa.eu/rapid/press-release_IP-14-2266_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2015a): Apoyo de los ministros de Justicia a la propuesta de la Comisión de fijar nuevas normas de protección de datos para impulsar el mercado único digital de la UE, Luxemburgo, 15 junio 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-5176_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2015b): La Comisión publica orientaciones sobre las transferencias transatlánticas de datos e insta al rápido establecimiento de un marco renovado tras la sentencia en el asunto Schrems, Bruselas, 6 de noviembre de 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-6015_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2015c): El acuerdo sobre la reforma de la protección de datos promovida por la Comisión reforzará el mercado único digital, Bruselas, 15 de diciembre de 2015. Disponible en Internet: http://europa.eu/rapid/press-release_IP-15-6321_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2016a): La Comisión Europea y los Estados Unidos acuerdan un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad UE - EE.UU., Estrasburgo, 2 de febrero de 2016. Disponible en Internet: http://europa.eu/rapid/press-release_IP-16-216_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2016b): Recuperar la confianza en los flujos de datos transatlánticos gracias a salvaguardias estrictas: la Comisión Europea presenta el Escudo de la privacidad UE-EE.UU., Bruselas, 29 de febrero de 2016. Disponible en Internet: http://europa.eu/rapid/press-release_IP-16-433_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2016c): La Comisión Europea pone en marcha el Escudo de la privacidad UE-EE.UU.: más protección para los flujos de datos transatlánticos, Bruselas, 12 de julio de 2016. Disponible en Internet: http://europa.eu/rapid/press-release_IP-16-2461_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2017a): Unión de la Seguridad: la Comisión cumple el compromiso contraído en materia de interoperabilidad de los sistemas de información de la UE, Bruselas, 29 de junio de 2017. Disponible en Internet: http://europa.eu/rapid/press-release_IP-17-1788_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2017b): Escudo de la privacidad UE-EE.UU.: un primer examen indica que funciona, pero que puede mejorarse, Bruselas, 18 de octubre de 2017. Disponible en Internet: http://europa.eu/rapid/press-release_IP-17-3966_es.htm.

COMISIÓN EUROPEA - Dirección General de Justicia y Consumidores (2016): Guía acerca del Escudo de Privacidad UE - EE.UU., págs. 24. Disponible en Internet: https://www.agpd.es/portalwebAGPD/noticias-inicio/common/pdf/2016/08_agosto/es_es_citizens-guide_en.pdf.

COMISIÓN EUROPEA - Hoja informativa (2018): Paquete de procedimientos de infracción correspondiente al mes de julio: principales decisiones, Bruselas, 19 de julio de 2018, MEMO/18/4486.

COMISIÓN EUROPEA - Press Release (2011): Propuesta de la UE sobre los datos de los pasajeros para combatir las formas graves de delincuencia y el terrorismo, Bruselas, 2 de febrero de 2011. Disponible en Internet: http://europa.eu/rapid/press-release_IP-11-120_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2010): La Comisión Europea adopta una estrategia para garantizar el respecto de la Carta de los Derechos Fundamentales de la UE, IP/10/1348, Bruselas, 19 de octubre de 2010. Disponible en Internet: http://europa.eu/rapid/press-release_IP-10-1348_es.htm.

COMISIÓN EUROPEA - Comunicado de prensa (2011): Entrada en funcionamiento de un sistema de visados más eficaz y seguro, Bruselas, 11 de octubre de 2011. Disponible en Internet: http://europa.eu/rapid/press-release_IP-11-1169_es.htm.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, An area of freedom, security and justice serving the citizen, (COM(2009)0262 final), Brussels, 10.6.2009. Disponible en Internet: https://ec.europa.eu/anti-trafficking/eu-policy/communication-commission-european-parliament-and-council-area-freedom-security-and-justice_en.

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia, Bruselas, 10.5.2005, COM(2005) 184 final. Disponible en Internet: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2009/7286.pdf?view=1

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia,

COM/2010/0385 final, Bruselas, 20.7.2010. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0385.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO (2016): Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, Bruselas, 6.4.2016. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016DC0205.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, COM/2007/0087 final, Bruselas, 7.3.2007. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007DC0087.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM/2013/0847 final, 27/11/2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52013DC0847.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018, COM(2018) 43 final, Bruselas, 24.1.2018. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52018DC0043.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Refuerzo de la cooperación en materia de aplicación de la ley en la UE: el Modelo Europeo para el Intercambio de Información (EIXM), COM/2012/0735 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0735.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Restablecer la confianza en los flujos de datos entre la UE y EE.UU., COM/2013/0846 final, 27/11/2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52013DC0846.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Segundo informe sobre la aplicación de la Estrategia de Seguridad Interior de la UE, COM(2013) 179 final, 10.4.2013. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52013DC0179.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO, Sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems), COM(2015) 566 final, Bruselas, 6.11.2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52015DC0566.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo, Bruselas, 20.4.2010, COM(2010) 171 final. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010DC0171.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Un enfoque global de la protección de los datos personales en la Unión Europea, COM(2010) 609 final, Bruselas, 4.11.2010. Disponible en Internet: http://ec.europa.eu/health/data_collection/docs/com_2010_0609_es.pdf.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Agenda Europea de Seguridad, COM(2015) 185 final, Estrasburgo, 28/4/2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52015DC0185.

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI, Bruselas, 25 de enero de 2012, COM/2012/09 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0009.

COMUNICACIÓN DE LA COMISIÓN, de 3 de marzo de 2010, denominada Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador [COM(2010) 2020 final – no publicada en el Diario Oficial]. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:em0028.

COMUNICACIÓN, DE 19 DE MAYO DE 2010, DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, titulada «Agenda digital para Europa» [COM(2010) 245 final - no publicada en el Diario Oficial]. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:si0016.

ESTADO DE LA UNIÓN 2016, Jean-Claude Juncker, presidente de la Comisión Europea, 14 de septiembre de 2016, págs. 68. Disponible en Internet: https://publications.europa.eu/es/publication-detail/-/publication/c9ff4ff6-9a81-11e6-9bca-01aa75ed71a1.

EUROPEAN COMMISSION - Directorate-General Justice, Freedom and Security (2010): Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Final Report, 20 January 2010, págs. 57. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

EUROPEAN COMMISSION - Fact Sheet (2015a): Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market, Brussels, 28 January 2015. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

EUROPEAN COMMISSION - Fact Sheet (2015b): Questions and Answers on the EU-US data protection "Umbrella agreement", Brussels, 8 September 2015. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

EUROPEAN COMMISSION - Fact Sheet (2016): EU-U.S. Privacy Shield: Frequently Asked Questions, Brussels, 12 july 2016. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm.

EUROPEAN COMMISSION - Memo (2013a): Informal Justice Council in Vilnius, Brussels, 19 July 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

EUROPEAN COMMISSION - Memo (2013b), LIBE Committee vote backs new EU data protection rules, Brussels, 22 October 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-923_es.htm.

EUROPEAN COMMISSION - Memo (2013c): Restoring Trust in EU-US data flows - Frequently Asked Questions, Brussels, 27 November 2013. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

EUROPEAN COMMISSION - Memo (2014): Frequently Asked Questions: The Data Retention Directive, Brussels, 8 April 2014. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-14-269_en.htm.

EUROPEAN COMMISSION - News (2016): Commission presents REFIT evaluation of the Visa Information System, 14 October 2016. Disponible en Internet: https://ec.europa.eu/home-affairs/what-is-new/news/news/2016/20161014_1_en.

EUROPEAN COMMISSION - Press Release (2014): A data protection compact for Europe, CEPS/Brussels, 28 January 2014. Disponible en Internet: http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm.

EUROPEAN COMMISSION - Speech (2014): Exchange of Views between Commissioner Dimitris Avramopoulos and MEPs at the LIBE Committee in the European Parliament, 03

December 2014. Disponible en Internet: http://europa.eu/rapid/press-release_SPEECH-14-2351_en.htm.

EUROPEAN COMMISSION - Statement (2015), Remarks by Commissioner Jourová after the launch of the Data protection regulation trilogue, Brussels, 24 June 2015. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm.

EUROPEAN COMMISSION - Statement (2016a): Statement by Commissioner Věra Jourová on the signature of the Judicial Redress Act by President Obama, Brussels, 24 February 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm.

EUROPEAN COMMISSION - Statement (2016b): Joint Statement on the final adoption of the new EU rules for personal data protection, Brussels, 14 April 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm.

EUROPEAN COMMISSION - Statement (2016c): Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting, Amsterdam, 2 June 2016. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-16-2040_en.htm.

EUROPEAN COMMISSION - Statement (2017): EU-Canada PNR agreement: Commission statement on the Opinion of the European Court of Justice, Brussels, 26 July 2017. Disponible en Internet: http://europa.eu/rapid/press-release_STATEMENT-17-2105_en.htm.

EUROPEAN COMMISSION (2014): Communication on data-driven economy, Brussels, 02/07/2014. Disponible en Internet: http://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy.

EUROPEAN COMMISSION (2016): EU-U.S. Privacy Shield fully operational from today, 01/08/2016. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=33704.

EUROPEAN COMMISSION - Press Release (2012): EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson, Memo/12/192, Brussels, 19 March 2012. Disponible en Internet: http://europa.eu/rapid/press-release_MEMO-12-192_en.htm?locale=en.

INFORME DE LA COMISIÓN - PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46 CE), COM/2003/0265 final. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52003DC0265.

INFORME DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO, Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), COM/2011/0225 final, 18/04/2011. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52011DC0225.

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre la evaluación del Sistema de Información Schengen de segunda generación (SIS II) de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n. 1987/2006 y el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, COM(2016) 880 final, Bruselas, 21.12.2016.

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE–EE.UU., COM/2017/0611 final, Bruselas, 18.10.2017.

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES presentado de conformidad con el artículo 29, apartado 2, de la Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0012.

INFORME SOBRE EL PRIMER INFORME SOBRE LA APLICACIÓN DE LA DIRECTIVA SOBRE PROTECCIÓN DE DATOS (95/46/CE), (COM (2003) 265 – 2003/2153(INI)), Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores, Final A5-

0104/2004, 24 de febrero de 2004. Disponible en Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2004-0104+0+DOC+XML+V0//ES.

PROPUESTA DE DECISIÓN DEL CONSEJO relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, COM(2011) 807 final, Bruselas, 23.11.2011. Disponible en Internet: http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1&year=2011&number=807&version=ALL&language=es.

DOCUMENTOS DEL CONSEJO EUROPEO

CONCLUSIONES Y PLAN DE ACCIÓN DEL CONSEJO EUROPEO EXTRAORDINARIO de 21 de septiembre de 2001, DOC/01/13, Bruselas, le 21 septiembre 2001. Disponible en Internet: http://europa.eu/rapid/press-release_DOC-01-13_es.htm.

CONSEJO EUROPEO - Comunicado de prensa (2015): Reforma de la protección de datos en la UE: el Consejo confirma el acuerdo con el Parlamento Europeo, 951/15, 18.12.2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/12/18-data-protection/.

CONSEJO EUROPEO (2014): Reunión extraordinaria del Consejo Europeo, Bruselas, 30.8.2014. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/european-council/2014/08/30/.

CONSEJO EUROPEO (2015): Consejo de Asuntos Exteriores, 19.1.2015, Sesión n. 3364, Bruselas, 19.1.2015. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/fac/2015/01/19/.

CONSEJO EUROPEO CONSEJO DE LA UNIÓN EUROPEA - Comunicado de prensa (2018): Acuerdo entre la Presidencia del Consejo y el Parlamento Europeo sobre eu-LISA, 285/18, 24.5.2018. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2018/05/24/eu-lisa-agreement-between-the-council-presidency-and-the-european-parliament/ [consulta: 05 de septiembre de 2018].

CONSEJO EUROPEO CONSEJO DE LA UNIÓN EUROPEA - Comunicados de prensa y declaraciones (2015): Reunión informal de los jefes de Estado o de Gobierno Bruselas, 12 de febrero de 2015 - Declaración de los miembros del Consejo Europeo, 12/2/2015. Disponible en Internet: http://www.consilium.europa.eu/es/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/.

CONSEJO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA (2015): Reunión informal de los jefes de Estado o de Gobierno, Bruselas, 12 de febrero de 2015. Disponible en Internet: http://www.consilium.europa.eu/es/meetings/european-council/2015/02/12/.

CONSEJO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA (2017): Reglamentación del uso de los datos del registro de nombres de pasajeros (PNR). Disponible en Internet: http://www.consilium.europa.eu/es/policies/fight-against-terrorism/passenger-name-record/.

DECISIÓN ADOPTADA DE COMÚN ACUERDO POR LOS REPRESENTANTES DE LOS GOBIERNOS DE LOS ESTADOS MIEMBROS REUNIDOS A NIVEL DE JEFES DE ESTADO O DE GOBIERNO RELATIVA A LA FIJACIÓN DE LAS SEDES DE DETERMINADOS ORGANISMOS Y SERVICIOS DE LAS COMUNIDADES EUROPEAS Y DE EUROPOL, *Diario Oficial*, n° C 323 de 30/11/1993, págs. 0001 - 0005.

EUROPEAN COUNCIL (2004): Declaration on Combating Terrorism, Brussels, 25 March 2004. Disponible en Internet: http://www.consilium.europa.eu/uedocs/cmsupload/decl-25.3.pdf.

EXTRAORDINARY COUNCIL MEETING - Justice, Home Affairs and Civil Protection, 12019/01 (Presse 327), Brussels, 20 September 2001. Disponible en Internet: http://www.consilium.europa.eu/uedocs/cmsUpload/12019.en1.pdf.

PROGRAMA DE ESTOCOLMO - UNA EUROPA ABIERTA Y SEGURA QUE SIRVA Y PROTEJA AL CIUDADANO, *Diario Oficial de la Unión Europea*, C 115 de 4.5.2010, págs. 1–38. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52010XG0504%2801%29.

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD), 15656/1/14, REV 1, Brussels, 28 November 2014. Disponible en Internet: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015656%202014%20REV%201.

PROPUESTA DE DECISIÓN MARCO DEL CONSEJO sobre utilización de datos del registro de nombres de los pasajeros (Passenger Name Record - PNR) con fines represivos, 2007/0237 (CNS), Bruselas, 6.11.2007, COM(2007) 654 final. Disponible en Internet: http://www.fomento.gob.es/AZ.BBMF.Web/documentacion/pdf/com2007_0654.pdf.

DOCUMENTOS DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (*EUROPEAN DATA PROTECTION SUPERVISOR - EDPS*)

DICTAMEN 3/2015. La gran oportunidad de Europa. Recomendaciones del SEPD sobre las opciones de la UE en cuanto a la reforma de la protección de datos, Bruselas, 28 de julio de 2015, págs. 17. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-10-09_GDPR_with_addendum_ES.pdf.

DICTAMEN DEL COMITÉ ECONÓMICO Y SOCIAL EUROPEO sobre la «Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)» COM(2012) 11 final - 2012/011 (COD), *Diario Oficial de la Unión Europea*, C 229, 31.7.2012, págs. 90–97. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012AE1303.

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la iniciativa del Reino de Bélgica, la República de Bulgaria, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos, la República de Austria, la República de Eslovenia, la República Eslovaca, la República Italiana, la República de Finlandia, la República Portuguesa, Rumanía y el Reino de Suecia con vistas a la adopción de la Decisión del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, *Diario Oficial de la Unión Europea*, C 169 de 21.7.2007, págs. 2–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0721(01).

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (COM (2005) 475 final), *Diario Oficial de la Unión Europea*, C 47 de 25.2.2006, págs. 27–47. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52006XX0225(01).

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo sobre el intercambio de información en virtud del principio de disponibilidad (COM(2005) 490 final), (2006/C 116/04), *Diario Oficial de la Unión Europea*,

C 116, 17.5.2006, págs. 8–17. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52006XX0517(01).

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final], *Diario Oficial de la Unión Europea*, C 298, 29.11.2005. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_ES.pdf.

DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, *Diario Oficial de la Unión Europea*, C 181, 22.6.2011, págs. 24–30. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52011XX0622%2802%29.

EDPS - Press Release (2012): EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice área, EDPS/02/12, Brussels, Wednesday 25 January 2012. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-02_EC_DP_Proposal_EN.pdf.

EDPS - Press Release (2016): Priorities for 2016: The EDPS as an advisor to the EU Institutions, EDPS/2016/02, Brussels, 7 January 2016. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-02-EDPS_PC_Prioritiesv2_EN.pdf.

EDPS - Press Release (2016): New Regulation boosts the roles of EDPS and Europol, 2016/09, Brussels, Thursday 19 May 2016. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-09-EDPS_Europol_EN.pdf.

EDPS - Press Release (2017): EDPS calls for consistency in EU approach to criminal récords, EDPS/2017/12, Brussels, 13 December 2017. Disponible en Internet: https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2017-12-ecris-tcn_en.pdf.

EDPS (2011a): Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", Brussels, 14 January 2011, págs. 36. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

EDPS (2011b): Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), Brussels, 31 May 2011. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf.

EDPS (2012): Opinion of the European Data Protection Supervisor on the data protection reform package, Brussels, 7 March 2012, págs. 75. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

EDPS (2013): Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, Brussels, 14 June 2013, págs. 26. Disponible en Internet:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf.

EDPS (2014): Press Statement: The CJEU rules that Data Retention Directive is invalid, 8 Apr 2014. Disponible en Internet: https://edps.europa.eu/press-publications/press-news/press-releases/2014/press-statement-cjeu-rules-data-retention_en.

EDPS (2015a): Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations, 27 July 2015, págs. 520. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf.

EDPS (2015b): Opinion 6/2015 A further step towards comprehensive EU data protection, 28 October 2015, págs. 12. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/15-10-28_directive_recommendations_en.pdf.

EDPS (2016a): Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences, Opinion 1/2016, 12 February 2016, págs. 21. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf.

EDPS (2016b): Opinion on the EU-U.S. Privacy Shield draft adequacy decisión, Opinion 4/2016, 30 May 2016, págs. 15. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf.

EDPS (2017a): Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, Brussels, 11 April 2017, págs. 29.

EDPS (2017b): EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 24 April 2017, págs. 40. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.

EDPS (2017c): EDPS Opinion on the proposal for a Regulation on the eu-LISA, Opinion 9/2017, 9 October 2017. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/17-10-10_eu-lisa_opinion_en_0.pdf.

EDPS (2017d): EDPS Opinion on the proposal for a Regulation on ECRIS-TCN, Opinion 11/2017, 12 December 2017. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/2017_0542_draft_opinion_ecris_tcn_revab_en.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR (2012): Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) (Recast version), Brussels, 5 September 2012, págs. 22. Disponible en Internet: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-09-05_EURODAC_EN.pdf.

EUROPEAN DATA PROTECTION SUPERVISOR - Press Release (2008): EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step, Brussels, Friday 28 November 2008. Disponible en Internet: https://edps.europa.eu/press-publications/press-news/press-releases/2008/edps-sees-adoption-data-protection-framework_en.

RESUMEN DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la nueva base jurídica del Sistema de Información de Schengen (2017/C 200/08), *Diario Oficial de la Unión Europea*, 23.6.2017.

RESUMEN EJECUTIVO DEL DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre el primer paquete de reformas del Sistema Europeo Común de Asilo (Reglamentos Eurodac, EASO y Dublín), *Diario Oficial de la Unión Europea*, C 9 de 12.1.2017, págs. 3–5. Disponible en Internet: http://eur-lex.europa.eu/legal-

content/ES/TXT/?uri=CELEX:52017XX0112(01)&qid=1504086633377#ntc4-C_2017009ES.01000301-E0004.

RESUMEN EJECUTIVO DEL SEGUNDO DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, *Diario Oficial de la Unión Europea*, C 392, 25.11.2015. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOC_2015_392_R_0009&from=ES.

SEGUNDO DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, *Diario Oficial de la Unión Europea*, C 91 del 26.4.2007, págs. 9–14. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0426(02).

SEPD (2016): Informe Anual 2015. Resumen ejecutivo, Luxemburgo, Oficina de Publicaciones de la Unión Europea, págs. 18. Disponible en Internet: https://edps.europa.eu/sites/edp/files/publication/ar2015_summary_es.pdf.

TERCER DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS sobre la propuesta de Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, (2007/C 139/01), *Diario Oficial de la Unión Europea*, C 139 del 23.6.2007, págs. 1–10. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007XX0623(01).

DOCUMENTOS DEL GRUPO DE TRABAJO DEL ARTÍCULO 29 (*ARTICLE 29 WORKING PARTY*)

ARTICLE 29 DATA PROTECTION WORKING PARTY - Press Release (2017): Preparation of the Privacy Shield annual Joint Review, 13 June 2017. Disponible en Internet: https://iapp.org/resources/article/preparation-of-the-privacy-shield-annual-joint-review/.

ARTICLE 29 DATA PROTECTION WORKING PARTY - Working Party on Police and Justice (2009): The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009, 02356/09/EN, WP 168, págs. 28. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2000): Working Document. Privacy on the Internet - An integrated EU Approach to On-line Data Protection, adopted on 21st November 2000, 5063/00/EN/FINAL, WP 37, págs. 99. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2001): Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, adopted on 14 December 2001, 0901/02/EN/Final, WP 53, págs. 4. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp53_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2003): Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, 11070/03/EN, WP 78, Adopted on 13 June 2003. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp78_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2004): Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, WP

87, Adopted on 29 January 2004. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp87_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2005): Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), 1868/05/EN, WP 113, adopted on 21st October 2005. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp113_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2006): Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 654/06/EN, WP 119, adopted on 25 March 2006. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp119_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2007): Opinion 4/2007 on the concept of personal data, Adopted on 20th June, 01248/07/EN, WP 136. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2010): Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, 00068/10/EN, WP 172, adopted on 13 July 2010. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp172_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2010b): Opinion 3/2010 on the principle of accountability, Adopted on 13 July 2010, 00062/10/EN, WP 173, págs. 4. Disponible en Internet: europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2011a): Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 00664/11/EN, WP 181, adopted on 5 April 2011, págs. 9. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp181_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2011b): Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, 01197/11/EN, WP187. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2012a): Letter from the Article 29 Working Party addressed to Members of the LIBE Committee of the European Parliament, Brussels, 6 January 2012. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2012b): Opinion 01/2012 on the data protection reform proposals, 00530/12/EN, WP 191, Adopted on 23 March 2012. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2012c): Opinion 08/2012 providing further input on the data protection reform discussions, 01574/12/EN, WP199, adopted on 05

October 2012. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013a): Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive, 00379/13/EN, WP 201, adopted on 26 February 2013. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013b): Opinion 02/2013 on apps on smart devices, adopted on 27 February 2013, 00461/13/EN, WP 202. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013c): Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, adopted on 2 April 2013, págs. 70. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013d): Explanatory Document on the Processor Binding Corporate Rules, Adopted on 19 April 2013. As last revised and adopted on 22 May 2015, 00658/13/EN, WP 204 rev.01. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp204.rev_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2014a): Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN, WP 215, Adopted on 10 April 2014. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2014b): Appendix: WP29 additional recommendations to strengthen personal data protection under the Safe Harbor Decision, Brussels, 10 April 2014. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2014c): Statement on the role of a risk-based approach in data protection legal frameworks, Adopted on 30 May 2014, 14/EN, WP 218. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015a): Letter on EU PNR, Brussels, 19 March 2015. Disponible en Internet: http://www.statewatch.org/news/2015/mar/eu-pnr-letter-art-29-wp-to-chair-libe.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015b): Annex to the letters: Core topics in view of the trilogue, 17 June 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015c): Propositions regarding the European Data Protection Board Internal Structure, 15 september 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150925_edpb_internal_structure.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015d): Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Adopted on 22 September 2015, 2588/15/EN, WP 232. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015e): Statement of the Article 29 Working Party, Brussels, 16 October 2015. Disponible en Internet:

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015f): Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 3211/15/EN, WP 233, Adopted on 01 December 2015. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2015g): Ms Ilze Juhansone, Ambassador Extraordinary and Plenipotentiary, Permanent Representative to the European Union. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjuhansone_en.pdf; Mr Jan Philipp Albrecht, Vice Chair Committee on Civil Liberties, Justice and Home Affairs. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_mralbrecht_en.pdf; Ms Věra Jourová, Commissioner for Justice, Consumers and Gender Equality European Commission. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_letter_from_the_art29_wp_on_trilogue_to_msjourova_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2016a): Statement of the Article 29 Working Party on the consequences of the Schrems judgment, Brussels, 3 February 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2016b): Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 16/EN, WP 237, Adopted on 13 April 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2016c): Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, 16/EN, WP 238, Adopted on 13 April 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2016d): Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, 26 de julio de 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/index_en.htm.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2017a): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, 17/EN, WP 248 rev.01, págs. 22. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2017b): Guidelines on the right to data portability, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017, 16/EN WP, 242 rev.01. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2017c): Guidelines on transparency under Regulation 2016/679, 17/EN, WP260, págs. 35. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

ARTICLE 29 WORKING PARTY - Press Release (2017): October 2017 Plenary Meeting. Disponible en Internet: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS (2000): Dictamen 4/2000 sobre el nivel de protección que proporcionan los "principios de puerto seguro", CA07/434/00/ES, WP 32, aprobado el 16 de mayo de 2000. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32es.pdf.

GRUPO DE PROTECCIÓN DE DATOS DEL ARTICULO 29 (2010): Dictamen 8/2010 sobre el Derecho aplicable, 0836-02/10/ES, WP 179, emitido el 16 de diciembre de 2010, págs. 39. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf.

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS (2013): Programa de trabajo 2014 - 2015, 02124/13/ES, WP 210, Adoptado el 3 de diciembre de 2013. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp210_es.pdf.

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1998): Documento de Trabajo - Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado por el Grupo de Trabajo el 24 de julio de 1998, WP 12. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf.

GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (1999): Dictamen 4/99. Inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales, aprobado el 7 de septiembre de 1999. Disponible en Internet: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26es.pdf.

GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (1999): Parere 1/99 riguardante il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità Europee e il Governo degli Stati Uniti, 5092/98/EN/finale, WP 15, adottato dal Gruppo di Lavoro il 26 gennaio 1999. Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp15_it.pdf.

DOCUMENTOS DE NACIONES UNIDAS (ONU)

DIRECTRICES PARA LA REGULACIÓN DE LOS ARCHIVOS DE DATOS PERSONALES INFORMATIZADOS, adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990. Disponible en Internet: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf.

Nota de 26 de febrero de 2014 adjunta a la Resolución aprobada por la Asamblea General el 18 de Diciembre de 2013. Disponible en Internet: http://www.ohchr.org/Documents/Issues/Privacy/NV.pdf.

NOTA DEL SECRETARIO GENERAL, Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/69/397, 23 de septiembre de 2014.

Disponible en Internet: http://repository.un.org/bitstream/handle/11176/158700/A_69_397-ES.pdf?sequence=6&isAllowed=y.

OBSERVACIONES GENERALES APROBADAS POR EL COMITÉ DE DERECHOS HUMANOS, Observación general núm. 16, Derecho a la intimidad (artículo 17). Disponible en Internet: https://conf-dts1.unog.ch/1%20SPA/Tradutek/Derechos_hum_Base/CCPR/00_2_obs_grales_Cte%20Der Hum%20%5BCCPR%5D.html.

RESOLUCIÓN 1373, aprobada por el Consejo de Seguridad en su 4385ª sesión, celebrada el 28 de septiembre de 2001, S/RES/1373 (2001), 28 de septiembre de 2001. Disponible en Internet: http://www.un.org/es/sc/ctc/resources/res-sc.html.

RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2013, 68/167, El derecho a la privacidad en la era digital, A/RES/68/167, 21 de enero de 2014, págs. 1-3. Disponible en Internet: http://www.un.org/es/comun/docs/?symbol=A/RES/68/167.

RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL EL 18 DE DICIEMBRE DE 2014, 69/166, El derecho a la privacidad en la era digital, A/RES/69/166, 10 de febrero de 2015. Disponible en Internet: http://www.un.org/es/comun/docs/?symbol=A/RES/69/166.

RESOLUCIÓN DEL CONSEJO DE DERECHOS HUMANOS SOBRE EL DERECHO A LA PRIVACIDAD EN LA ERA DIGITAL, A/HRC/28/L.27, 24 de marzo de 2015. Disponible en Internet: http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/28/L.27&referer=/english/&Lang=S.

RESOLUTION ADOPTED BY THE HUMAN RIGHTS COUNCIL ON 23 MARCH 2017, The right to privacy in the digital age, A/HRC/RES/34/7, 7 April 2017.

RESUMEN DE LA MESA REDONDA DEL CONSEJO DE DERECHOS HUMANOS sobre el derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, A/HRC/28/39, 19 de diciembre de 2014, págs. 1-18. Disponible en Internet: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39&referer=http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx&Lang=S.

DOCUMENTOS ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (OCDE)

«Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales», en *OCDE Online Bookshop*, 2002, págs. 12. Disponible en internet: http://www.oecd.org/sti/ieconomy/15590267.pdf.

DIRECTRICES DE LA OCDE PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN: HACIA UNA CULTURA DE SEGURIDAD, adoptados como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002, págs. 12. Disponible en internet: https://www.oecd.org/sti/ieconomy/34912912.pdf.

DIRECTRICES RELATIVAS A LA PROTECCIÓN DE LA INTIMIDAD Y DE LA CIRCULACIÓN TRANSFRONTERIZA DE DATOS PERSONALES, 23 de septiembre de 1980.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79], págs. 11-37. Disponible en internet: https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

DOCUMENTOS DEL CONSEJO DE EUROPA

AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), Abridged Report 3 rd meeting Agora - Strasbourg 1 - 3 December 2014, CAHDATA(2014)RAP03Abr. Disponible en Internet: https://rm.coe.int/16806b7e90.

AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), Abridged Report, Strasbourg 15-16 June 2016, CAHDATA(2016)RAPAbr. Disponible en Internet: https://rm.coe.int/16806b7e90.

CONVENIO PARA LA PROTECCIÓN DE LOS DERECHOS HUMANOS Y DE LAS LIBERTADES FUNDAMENTALES, Roma, 4.XI.1950.

MODERNISED CONVENTION for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018). Disponible en Internet: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

RECOMENDACIÓN N. R (95) 4 DEL COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA en materia jurídica a los estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, en especial con relación a los servicios telefónicos (Adoptada por el Comité de Ministros el 7 de febrero de 1995, durante la 528ª reunión de los Delegados de los Ministros). Disponible en Internet: http://www.informatica-juridica.com/anexos/recomendacion-no-r-95-4-del-comite-de-ministros-del-consejo-de-europa-en-materia-juridica-a-los-estados-miembros-sobre-la-proteccion-de-los-datos-de-caracter-personal-en-el-ambito-de-los-servicios-de/.

RECOMMENDATION REC(87)15 to member states regulating the use of personal data in the police sector, Strasbourg, 17 September 1987.

RESERVATIONS AND DECLARATIONS FOR TREATY N.005 - Convention for the Protection of Human Rights and Fundamental Freedoms. Disponible en Internet: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations?p_auth=IRgBNXHj.

OTROS DOCUMENTOS

«Acuerdo sobre el Espacio Económico Europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:em0024.

«Adequacy of the protection of personal data in non-EU countries», en *European Commission*. Disponible en Internet: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

«Apple contra el FBI: la delgada línea entre privacidad y seguridad pública», en *Euronews*, 02/03/2016. Disponible en Internet: http://es.euronews.com/2016/03/02/apple-contra-el-fbi-la-delgada-linea-entre-privacidad-y-seguridad-publica.

«Cameron plantea prohibir WhatsApp en Reino Unido tras los ataques en París», en *Diario ABC*, 13/01/2015. Disponible en Internet: http://www.abc.es/internacional/20150113/abci-cameron-whatsapp-kouachi-201501131107.html.

«Código de visados», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:jl0028.

«Comentario a la Directiva (UE) 2016/680, de 27 de abril, sobre protección de datos en el ámbito de las infracciones penales», en *Diario La Ley*, Editorial La Ley, n. 8756, 6 de mayo de 2016.

«Conclusiones VIII Foro de la Privacidad del Data Privacy Institute», en *Lefebvre - El Derecho*, Madrid, 17.02.16. Disponible en Internet:

http://tecnologia.elderecho.com/tecnologia/privacidad/Conclusiones-VIII-Foro-Privacidad-Privacy-Data-Privacy-Institute_0_919500062.html.

«Consolidated Annual Activity Report (CAAR) 2017», en *EUROPOL*. Disponible en Internet: https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2017.

«Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016)», en *Noticias Jurídicas*, 04/05/2016. Disponible en Internet: http://noticias.juridicas.com/actualidad/noticias/11050-contenido-y-novedades-del-reglamento-general-de-proteccion-de-datos-de-la-ue-reglamento-ue-2016-679-de-27-de-abril-de-2016/.

«Creación de un Sistema de Información de Visados (VIS) - primera etapa», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14516.

«DRI brings legal action over mass surveillance», en *Digital Rights Ireland*, 14 SEP 2006. Disponible en Internet: https://www.digitalrights.ie/dri-brings-legal-action-over-mass-surveillance/.

«EDRi's suggested amendments to the Commission's. Proposal for a Regulation on the Protection of individuals with regard to the processing of personal data, and the free movement of such data (General Data Protection Regulation) COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)», en *European Digital Rights (EDRi)*, 12/12/2012, págs. 122. Disponible en Internet: http://protectmydata.eu/topics/edris-proposed-amendments/.

«El efecto directo del Derecho europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14547.

«El espacio y la cooperación Schengen», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l33020.

«El Gobierno aprueba el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal», en *Diario la Ley*, 10-11-2017.

«El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales a la abogacía», en *Noticias Jurídicas*, 30/04/2016. Disponible en Internet: http://noticias.juridicas.com/actualidad/noticias/11047-el-nuevo-reglamento-europeo-de-proteccion-de-datos:-un-texto-complejo-que-abre-nuevas-perspectivas-profesionales-a-la-abogacia/.

«EU Data Protection Reform: The Directive on police, justice and criminal matters», en *Youtube*, video, 7.12.2015. Disponible en Internet: https://www.youtube.com/watch?v=_Q19JtF3ieI&feature=youtu.be.

«EU justice ministers agreed to seek better data protection», en *Lithuanian Presidency of the EU Council 2013*, 19 July 2013. Disponible en Internet: http://www.eu2013.lt/en/news/pressreleases/eu-justice-ministers-agreed-to-seek-better-data-protection-.

«EU: Data protection proposal in a muddle - member states divided - three Council working parties discussing the draft measure», en *Statewatch News online*, 2006. Disponible en Internet: http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm.

«EUROPOL pone en marcha el Centro Europeo Contra el Terrorismo (ECTC)», en *EUROPOL y Ministerio del Interior*. Disponible en Internet: http://www.dsn.gob.es/es/actualidad/sala-prensa/europol-pone-marcha-centro-europeo-contra-terrorismo-ectc.

«Europol: Oficina Europea de Policía», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l14005b.

«Europol's Internet Referral Unit to combat terrorist and violent extremist propaganda», en *Press Release Europol*, 01 July 2015. Disponible en Internet: https://www.europol.europa.eu/newsroom/news/europol%E2%80%99s-internet-referral-unit-to-combat-terrorist-and-violent-extremist-propaganda.

«EU-US data protection/Safe Harbour», en *The Greens/European Free Alliance*, 02.02.2016. Disponible en Internet: https://www.greens-efa.eu/en/article/eu-us-data-protection-safe-harbour/.

«Francia: Nueva ley de vigilancia, duro golpe para los derechos humanos», en *Amnistía Internacional España*, 24 de julio de 2015. Disponible en Internet: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/francia-nueva-ley-de-vigilancia-duro-golpe-para-los-derechos-humanos/.

«Francia: Nueva ley de vigilancia, duro golpe para los derechos humanos», en *Amnistía Internacional España*, 24 de julio de 2015. Disponible en Internet: https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/francia-nueva-ley-de-vigilancia-duro-golpe-para-los-derechos-humanos/.

«Garante privacy Ue, Pnr è infortunio normativo. Buttarelli, misura costosissima e richiede tempi semi-biblici», en *Ansa.it*, 14 aprile 2016. Disponible en Internet: http://www.ansa.it/europa/notizie/rubriche/altrenews/2016/04/14/garante-privacy-ue-pnr-e-infortunio-normativo_d9014be4-028e-477a-9479-18cc06f72d51.html.

«GDPR, cosa cambia con le nuove linee guida su trasparenza e responsabilizzazione», en *AgendaDigitale.eu*, 15 Dic 2017. Disponible en Internet: https://www.agendadigitale.eu/sicurezza/gdpr-cosa-cambia-con-le-nuove-linee-guida-su-trasparenza-e-responsabilizzazione/.

«Il nuovo Regolamento Eurodac (603/2013) per la raccolta e comparazione delle impronte digitali si applica a partire da oggi» en *Asilo in Europa*, 20 luglio 2015. Disponible en Internet: http://www.asiloineuropa.it/2015/07/20/il-nuovo-regolamento-eurodac-6032013-per-la-raccolta-e-comparazione-delle-impronte-digitali-si-applica-a-partire-da-oggi/.

«Il Regno Unito verso la sorveglianza totale: "Un attacco alla democrazia"», en *Valigia Blu*, 3 de diciembre 2016. Disponible en Internet: http://www.valigiablu.it/uk-legge-sorveglianza/.

«Investigatory Powers Bill: Commons stages», en *Parliament.uk*, 30 November 2016. Disponible en Internet: http://www.parliament.uk/business/news/2016/march/investigatory-powers-bill-commons-second-reading/.

«Is the new EU-US PNR Agreement acceptable?», en *European Digital Rights (EDRi)*, 2012, págs. 2. Disponible en Internet: https://edri.org/files/2012EDRi_US_PNRcomments.pdf.

«La Commissione propone di rafforzare il sistema d'informazione Schengen», en *Rappresentanza in Italia della Commissione europea*, 21-12-2016. Disponible en Internet: https://ec.europa.eu/italy/news/20161221_sis_it.

«La obligación de conservación de datos impuesta por un Estado debe estar sujeta a estrictas garantías», en *Law&Trends*, 19/07/2016. Disponible en Internet: http://www.lawandtrends.com/noticias/ue-internacional/la-obligacion-de-conservacion-de-datos-impuesta.html.

«La protección de los derechos fundamentales en la Unión Europea», en en *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo. Disponible en Internet: http://www.europarl.europa.eu/factsheets/es/sheet/146/la-proteccion-de-los-derechos-fundamentales-en-la-union-europea.

«Las Autoridades europeas de Protección de Datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el Puerto Seguro», en *AGPD*, Madrid, 19 de octubre de 2015. Disponible en Internet: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php.

«Los ministros de Interior europeos acuerdan revisar el tratado de Schengen», en *El Confidencial*, 11.01.2015. Disponible en Internet: http://www.elconfidencial.com/mundo/2015-01-11/europa-y-estados-unidos-acuerda-en-paris-reforzar-la-lucha-contra-el-terrorismo_619798/.

«Los proveedores de servicios de comunicaciones no están obligados a una conservación general de datos de sus usuarios», en *Diario La Ley*, 21-12-2016. Disponible en Internet:

http://diariolaley.laley.es/home/NE0001175792/20161221/Los-proveedores-de-servicios-de-comunicaciones-no-estan-obligados-a-una-conserva.

«Los servicios secretos alemanes espiaron a medios extranjeros, según 'Der Spiegel'», en *El Confidencial*, 24.02.2017. Disponible en Internet: https://www.elconfidencial.com/mundo/2017-02-24/servicios-secretos-alemania-espiarion-medios-extranjeros-spiegel_1338357/.

«Mercado único digital. Derribar barreras para aprovechar las posibilidades que ofrece internet», en *Comisión Europea*. Disponible en Internet: https://ec.europa.eu/commission/priorities/digital-single-market_es.

«Obligación por parte de los transportistas aéreos de comunicar los datos sobre los pasajeros», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=URISERV:l14582.

«Ordinary legislative procedure», en *European Parliament*. Disponible en Internet: http://www.europarl.europa.eu/external/html/legislativeprocedure/default_en.htm.

«Pacchetto protezione dati in G.U.U.E.: Soro, giornata importante per i cittadini europei. Disciplina uniforme contro ogni barriera», en *Garante per la protezione dei dati personali*, Roma, 4 maggio 2016. Disponible en Internet: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4966337.

«Più tutele per lo scambio di dati tra Use Ue a fini giudiziari», en *Eunews*, 1 dicembre 2016. Disponible en Internet: http://www.eunews.it/2016/12/01/piu-tutele-per-lo-scambio-di-dati-tra-use-ue-fini-giudiziari/73356.

«Press Release: Permission Granted for Judicial Review of DRIPA», en *Open Rights Group*, December 08, 2014. Disponible en Internet: https://www.openrightsgroup.org/press/releases/press-release:-permission-granted-for-judicial-review-of-ripa.

«Primacía del Derecho europeo», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14548.

«PRISM Scandal - EPP Group to push introduction of 'Anti-net tapping clause'», en *EPP Group*, 19.06.2013. Disponible en Internet: http://www.eppgroup.eu/press-release/PRISM%3A-we-want-introduction-of-'Anti-net-tapping-clause'.

«Procedimiento legislativo ordinario. Fase 2: Primera lectura», en *Consejo de la Unión Europea*. Disponible en Internet: http://www.consilium.europa.eu/es/council-eu/decision-making/ordinary-legislative-procedure/first-reading/.

«Profundización de la cooperación transfronteriza (Decisión Prüm)», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:jl0005#KEYTERMS.

«Proposal for a Regulation on Privacy and Electronic Communications», en *European Commission*, 10 January 2017. Disponible en Internet: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

«Protección de los datos personales», en *EUR-Lex*. Disponible en Internet: https://eur-lex.europa.eu/legal-content/ES/LSU/?uri=CELEX:31995L0046.

«Rapporto 2016 dell'Osservatorio sul rispetto dei diritti fondamentali in Europa», en *Fondazione Basso*, 2016, págs. 54.

«Refuerzo del Sistema de Información de Schengen para mejorar la lucha contra el terrorismo y la delincuencia transfronteriza», en *Diario La Ley*, Wolters Kluwer, 20-1-2017.

«Reglamento General de Protección de Datos», en *AEPD*. Disponible en Internet: https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php.

«Safe-Harbor - Update (26.10.2015)», Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder. Disponible en Internet: https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.html.

«Secure Information Exchange Network Application (Siena)», en *europol.europa.eu*. Disponible en Internet: https://www.europol.europa.eu/content/page/siena-1849.

«Sistema de información Schengen de segunda generación (SIS II) - reglamento del antiguo primer pilar», en *EUR-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14544#KEYTERMS.

«Sistema de Información Schengen de segunda generación (SIS II): decisión del antiguo 3er pilar», en *EU-Lex*. Disponible en Internet: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l14569.

«Sistema de Información Schengen de segunda generación (SIS II)», en *Agencia Española de Protección de Datos*. Disponible en Internet: http://www.agpd.es/portalwebAGPD/internacional/Europa/Cooperacion_Policial_Judicial/Sistema_de_Informacion_SCHENGEN/index-ides-idphp.php.

«Sistema Europeo de Información de Antecedentes Penales (ECRIS)», en *Portal Europeo de e-Justicia*. Disponible en Internet: https://e-justice.europa.eu/content_criminal_records-95-es.do.

«Transatlantic coalition of civil society groups: Privacy Shield is not enough - renegotiation is needed (Privacy Shield Letter by 27 civil society groups)», en *European Digital Rights (EDRi)*, march 16, 2016. Disponible en Internet: https://edri.org/transatlantic-coalition-of-civil-society-groups-privacy-shield-is-not-enough-renogitation-is-needed/.

«Transferencias internacionales de datos», en *AGPD*. Disponible en Internet: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php.

«Tribunal Constitucional chumba acesso das secretas a dados bancários e de comunicações», en *observador*. Disponible en Internet: http://observador.pt/2015/08/27/tribunal-constitucional-chumba-acesso-das-secretas-a-dados-bancarios-e-de-comunicacoes/.

«Una consultora que trabajó para Trump robó a Facebook datos de 50 millones de usuarios para influir en las elecciones», en *ABC.es*, 18/03/2018. Disponible en Internet: https://www.abc.es/internacional/abci-trump-robo-facebook-datos-50-millones-usuarios-para-influir-elecciones-201803172343_noticia.html.

«Unión de la Seguridad: la Comisión presenta nuevas medidas para proteger mejor a los ciudadanos de la UE», en *Diario La Ley*, Wolters Kluwer, 21-11-2017.

«US on its way to adopt Judicial Redress Act and hopefully facilitate transfers from the EU», en *Privacy Laws & Business*, 21/10/2015. Disponible en Internet: https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2015/10/US-on-its-way-to-adopt-Judicial-Redress-Act-and-hopefully-facilitate-transfers-from-the-EU/.

«Valls: "El terrorismo formará parte de nuestro día a día durante mucho tiempo"», en *RTVE.es/EFE*, 17.07.2016. Disponible en Internet: http://www.rtve.es/noticias/20160717/valls-terrorismo-formara-parte-nuestro-dia-dia-durante-mucho-tiempo/1372081.shtml.

Decision by the supreme supervisory authorities for data protection in the nonpublic sector on 28/29, April 2010 in Hannover [revised version of 23 August 2010]. Disponible en Internet: https://www.datenschutzzentrum.de/internationaler-datenverkehr/Resolution_DuesseldorfCircle_DE%20DPAs_rev.EN.pdf.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit - Press release: Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe, Bremen/Bremerhaven, 24 July 2013. Disponible en Internet: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.

Documents and Public Comments Provided through the Duration of the Safe Harbor Negotiations (November 1998 - June 2000), june 9, 2000. Disponible en Internet: https://build.export.gov/main/safeharbor/eu/eg_main_018496.

FEDERAL TRADE COMMISSION - press releases (1999): "Self-Regulation and Privacy Online", FTC Report to Congress, July 13, 1999. Disponible en Internet:

https://www.ftc.gov/news-events/press-releases/1999/07/self-regulation-and-privacy-online-ftc-report-congress.

Home Office, *Data Retention and Investigatory Powers Act 2014: Further information*, 10 July 2014. Disponible en Internet: https://www.gov.uk/government/publications/the-data-retention-and-investigatory-powers-bill.

INCLO International Network of Civil Liberties Organizations, *Vigilancia y democracia*, págs. 122. Disponible en Internet: https://www.inclo.net/pdf/surveillance-and-democracy-sp.pdf.

Modernisation of Convention 108. Disponible en Internet: https://www.coe.int/en/web/data-protection/convention108/modernised.

Office of the Director of National Intelligence, Office of General Counsel, *Annex VI*, Washington, DC 20511, 22 de febrero de 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf.

PRIME MINISTER'S OFFICE - Speech, *PM and Deputy PM Speech on Emergency Security Legislation*, 11 July 2014. Disponible en Internet: https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation.

Profiling. Protecting citizens' rights fighting illicit profiling, project funded by the European Commission, DG Justice, under the Fundamental Rights and Citizenship programme, 2014, págs. 192. Disponible en Internet: http://www.unicri.it/news/files/Profiling_final_report_2014.pdf.

SPECIAL EUROBAROMETER 359, Attitudes on Data Protection and Electronic Identity in the European Union, Conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre, Brussels, June 2011, págs. 330. Disponible en Internet: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf.

THE SECRETARY OF STATE, *Annex III*, Washington, February 22, 2016. Disponible en Internet: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf.

THE WHITE HOUSE - Office of the Press Secretary, Executive Order: Enhancing Public Safety in the Interior of the United States, January 25, 2017. Disponible en Internet: https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

THE WHITE HOUSE - Office of the Press Secretary, Presidential Policy Directive - Signals Intelligence Activities, January 17, 2014. Disponible en Internet: https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

Visa Information System (VIS). Disponible en Internet: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en.

NORMATIVA Y JURISPRUDENCIA ESTADOS DE LA UNIÓN EUROPEA Y DE EE.UU.

ESPAÑA

Instrumento de ratificación de España del Convenio relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, hecho en Prüm el 27 de mayo de 2005, *Boletín Oficial del Estado*, núm. 307, lunes 25 diciembre 2006, págs. 45524-45534.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, publicado en *BOE*, núm. 251, de

19/10/2007. Disponible en Internet: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243.
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

ITALIA

CORTE DI CASSAZIONE, Sezione VI, 26 maggio 2015-26 giugno 2015, n. 27100. Disponible en Internet: http://www.penale.it/page.asp?IDPag=1201.
DECRETO LEGISLATIVO 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali. Disponible en Internet: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248.
DECRETO LEGISLATIVO 18 maggio 2018, n. 51. Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. (18G00080) (*GU Serie Generale* n. 119 del 24-05-2018).
DECRETO LEGISLATIVO 21 maggio 2018, n. 53. Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004. (18G00081) (*GU Serie Generale* n.120 del 25-05-2018).
Legge 30 giugno 2009, n. 85, *Gazzetta Ufficiale*, n. 160 del 13-7-2009 - Suppl. Ordinario n. 108.
Legge 21 febbraio 1989, n. 98. Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981, (*GU Serie Generale* n. 66 del 20-03-1989 - Suppl. Ordinario n. 19), entrata in vigore della legge 21/3/1989.
Ley de 31 de diciembre de 1996, n. 675. "*Codice in materia di protezione dei dati personali*", adoptado por Decreto Legislativo de 30 de junio 2003, n. 196.

REINO UNIDO

Anti-Terrorism, Crime and Security Act 2001, 14th December 2001. Disponible en Internet: http://www.legislation.gov.uk/ukpga/2001/24.
ROYAL COURTS OF JUSTICE, *David Davis and others -v- Secretary of State for the Home Department*, n. EWHC 2092, Case N.: CO/3665/2014, CO/3667/2014, CO/3794/2014, 17 July 2015. Disponible en Internet: https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/.

ALEMANIA

Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird, BGBl. I, 27/2011.
BVerfG · Urteil vom 15. Dezember 1983 · Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil). Disponible en Internet: https://openjur.de/u/268440.html.
Counter-terrorism database in its fundamental structures compatible with the Basic Law, but not regarding specific aspects of its design, Press Release N. 31/2013 of 24 April 2013. Disponible en Internet:

https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2013/bvg13-031.html.

Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten', 27 May 2015.

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU). Disponible en Internet: https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2017/0301-0400/0332-17.html.

Tribunal Constitucional Federal de Alemania (*Bundesverfassungsgericht*), 1 BvR 256/08, de 2 de marzo de 2010.

FRANCIA

Code des postes et des communications électroniques, Version consolidée au 26 octobre 2016. Disponible en Internet: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987.

DÉCRET n. 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

Décret n. 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique. Disponible en Internet: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477&dateTexte=&categorieLien=id.

LOI n. 2015-912 du 24 juillet 2015 relative au renseignement.

LOI n. 55-385 du 3 avril 1955 relative à l'état d'urgence, Version consolidée au 26 novembre 2015. Disponible en Internet: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000695350&dateTexte=20151126.

RUMANÍA

Tribunal Constitucional Federal de Rumanía (Curtea Constituțională a României), n. 1258, de 8 de octubre de 2009.

REPÚBLICA CHECA

Tribunal Constitucional de la República Checa (*Ústavní soud České republiky*), n. 94/2011 Rec., de 22 de marzo de 2011.

EE.UU.

18 U.S. Code § 2702 (b) (7) - Voluntary disclosure of customer communications or records. Disponible en Internet: https://www.law.cornell.edu/uscode/text/18/2702.

Aviation and Transportation Security Act, Public Law 107–71, 107th Congress, nov. 19, 2001. Disponible en Internet: https://www.tsa.gov/sites/default/files/aviation_and_transportation_security_act_atsa_public_law_107_1771.pdf.

H.R.1428 - Judicial Redress Act of 2015, Public Law N.: 114-126 (02/24/2016). Disponible en Internet: https://www.congress.gov/bill/114th-congress/house-bill/1428.

S.2588 - Cybersecurity Information Sharing Act of 2014, 113th Congress (2013-2014). Disponible en Internet: https://www.congress.gov/bill/113th-congress/senate-bill/2588.

Statement From U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield, February 2, 2016. Disponible en Internet: https://www.commerce.gov/news/press-releases/2016/02/statement-us-secretary-commerce-penny-pritzker-eu-us-privacy-shield.